2011-06

Implementing Joint Battlespace Awareness ISR Integration Capability (JBAIIC) test bed architecture a crime-reduction strategy in Salinas, California

Dubay, Jerome E.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTING JOINT BATTLESPACE AWARENESS ISR INTEGRATION CAPABILITY (JBAIIC) ARCHITECTURE: A CRIME-REDUCTION STRATEGY IN SALINAS, CALIFORNIA

by

Jerome E. Dubay

June 2011

Thesis Advisor:	Douglas J. MacKinnon
Second Readers:	Brian P. Wood
	Victor R. Garza

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Implementing Joint Battlespace Awareness ISR Integration Capability (JBAIIC) Test Bed Architecture: A Crime Reduction Strategy in Salinas, California		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jerome E. Dubay			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number: N/A			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Planning, executing, and monitoring Command and Control (C2) is difficult to accomplish on many levels, yet much has been learned in terms of applying improved technology to achieve it. This knowledge seems directly transferable from the battlefield to any environment requiring improved C2. This thesis demonstrates how DoD Information Technology architecture can be used to enhance C2 of a medium sized urban police department (PD) struggling to reduce gang violence in the face of significant resource reductions. Using a field demonstration, researchers demonstrate how a Common Tactical Picture (CTP) can improve officer effectiveness at the Salinas Police Department (SPD) in Salinas, California. Upon completion of the field demonstration, comparisons are made between the existing information and communications architecture of SPD and a baseline Joint Battlespace Awareness ISR Integration Capability (JBAIIC) testbed architecture to identify capability gaps that limit SPD's ability to more effectively combat violent crime. Based on this analysis, a Technology Implementation Plan (TIP) is created, identifying courses of action available to SPD so that current and upcoming technological initiatives can be properly implemented—and potentially transferred to other municipal Law Enforcement agencies needing to extend their own their limited resources.

14. SUBJECT TERMS Information Technology, Technology Integration, Common Operational Picture (COP), Common Tactical Picture (CTP), Enterprise Architecture, Situational Awareness (SA), Police, Computer Aided Dispatch, Predictive Policing, Information Architecture, Police			**15. NUMBER OF PAGES** 129
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPLEMENTING JOINT BATTLESPACE AWARENESS ISR INTEGRATION CAPABILITY (JBAIIC) TEST BED ARCHITECTURE: A CRIME-REDUCTION STRATEGY IN SALINAS, CALIFORNIA

Jerome E. Dubay
Lieutenant Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2011

Author: Jerome E. Dubay

Approved by: Douglas J. MacKinnon, PhD
Thesis Advisor

Brian P. Wood
Second Reader

Victor R. Garza
Second Reader

Dan Boger, PhD
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Planning, executing, and monitoring Command and Control (C2) is difficult to accomplish on many levels, yet much has been learned in terms of applying improved technology to achieve it. This knowledge seems directly transferable from the battlefield to any environment requiring improved C2. This thesis demonstrates how DoD Information Technology architecture can be used to enhance C2 of a medium sized urban police department (PD) struggling to reduce gang violence in the face of significant resource reductions. Using a field demonstration, researchers demonstrate how a Common Tactical Picture (CTP) can improve officer effectiveness at the Salinas Police Department (SPD) in Salinas, California. Upon completion of the field demonstration, comparisons are made between the existing information and communications architecture of SPD and a baseline Joint Battlespace Awareness ISR Integration Capability (JBAIIC) testbed architecture to identify capability gaps that limit SPD's ability to more effectively combat violent crime. Based on this analysis, a Technology Implementation Plan (TIP) is created, identifying courses of action available to SPD so that current and upcoming technological initiatives can be properly implemented—and potentially transferred to other municipal Law Enforcement agencies needing to extend their own their limited resources.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AT-FLIR	Advanced Targeting—Forward Looking Infrared Radar
BFT	Blue Force Tracking
BGAN	Broadband Global Area Network
BPR	Business Process Reengineering
C2	Command and Control
CAD	Computer Aided Dispatch
CCTV	Closed Circuit Television
CFE	Coalition Four Eyes
CIO	Chief Information Officer
CLETS	California Law Enforcement Telecommunications System
COA	Courses of Action
COI	Community Of Interest
CONUS	Continental United States
COP	Community Oriented Policing
COPS Grant	Community Oriented Policing Grant
CoT	Cursor on Target
CTP	Common Tactical Picture
DA	Defense Analysis
DDTE	Distributed Development and Test Enterprise
DISE	Distributed Information Systems Experimentation Research Group
DoD	Department of Defense
DOJ	Department of Justice
EA	Enterprise Architecture
EP	External Processes
FCC	Federal Communications Commission
FI	Field Interview
FLIR	Forward Looking Infrared Radar
FMV	Full Motion Video
GIS	Graphical Information System
GLS	Gunshot Location System

GPS	Global Positioning System
HQ	Headquarters
I-CTP	Interactive Common Tactical Picture
INMARSAT	International Maritime Satellite Communications
IP	Internet Protocol
IP	Internal Procedure
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITD	Information Technology Department
JBAIIC	Joint Battlespace Awareness ISR Integration Capability Testbed
JMSM	Joint Mission Support Module
JRV	Joint Reconfigurable Vehicle
LAN	Local Area Network
LMRS	Land Mobile Radio System
LOS	Line-of-sight
Mb	Megabyte
MCP	Mobile Command Post
MCV	Mobile Command Vehicle
MDSD	Mobile Data Sharing Device
MDT	Mobile Data Terminal
NCIC	National Criminal Information Center
NGEN	Next Generation Radio
NIPRNet	Non-Classified Internet Protocol Router Network
NOC	Network Operations Center
NPS	Naval Postgraduate School
PD	Police Department
PhD	Doctor of Philosophy
PRC-117G	Tactical Radio made by Harris Radio
PRC-152	Tactical Radio made by Harris Radio
RF	Radio Frequency
RMS	Records Management System
ROVER	Remotely Operated Video Enhanced Receiver

SA	Situational Awareness
SAR	Synthetic Aperture Radar
SFD	Salinas Fire Department
SIPRNet	Secret Internet Protocol Router Network
SNC	Sierra Nevada Corporation
SNS	Secure Network Server
SPD	Salinas Police Department
TacSat	Tactical Satellite
TIP	Technology Implementation Plan
TOC w/ I-CTP	Tactical Operations Center with Interactive Common Tactical Picture
TWG	Technical Working Group
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicles
UGS	Unattended Ground Sensor
UHF	Ultra High Frequency
USAF	United States Air Force
USJFCOM	United States Joint Forces Command
VAP	Virtual Access Point
VHF	Very High Frequency
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This research effort would not have been possible without a tremendous amount of dedication and professionalism from many people. I first want to thank the Salinas Police Department for allowing the Naval Postgraduate School to investigate the many complicated aspects of their day-to-day operations. Secondly, the team of professionals that make up the DISE research group and JBAIIC experimentation team were constantly open to my questions and helping me stay on track throughout this process. Specifically, I would like to thank my advisors Dr. Doug MacKinnon and Mr. Brian Wood and for the countless hours they dedicated to teaching me about the technologies involved in this thesis as well as the professional critiques of the many drafts of this paper. Additionally, this paper would not have been possible without the technical knowledge and personal assistance of Mr. Bob Garza. I have your phone number etched in my brain forever. Finally, and most importantly, I want to thank my wife, Katie, and our three little monkeys at home, Maryanna, Tommy, and Baby Rose who sacrificed many weekends and outings without daddy, which enabled me to complete this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

1. Salinas California and Gang Violence

In 2009, the homicide per capita rate ranked the city of Salinas fourth in the State of California (Fetherolf, 2010). Despite a nationwide decrease in homicides from 2006 to 2009, the homicide rate in Salinas increased during this same period and, by 2009, was four times the national average (Dept of Justice, 2009). Additionally, of the 29 homicides in 2009, all were gang related (Lorentz, 2010).

To address this problem, the Salinas Police Department (SPD) needs modern technology supported by an information and communications architecture (herein referred to as 'architecture') capable of providing police a secure means to access and distribute information. Specifically, this architecture must be capable of combating Salinas' most significant threat: gang violence. This architecture cannot focus solely on the adoption of new technology but must also address how the entire spectrum of SPD's Information Technology (IT) relates to both its Enterprise Architecture (EA) and current business processes. Unfortunately, SPD is not supported at present by such an architecture.

The Information and Communications architecture of SPD is old and antiquated and consists of many stand-alone information silos that do not communicate with other essential systems (Officer #1, personal communication, February 10, 2011). For example, the fingerprint, mug shot, and Records Management System (RMS) databases are not linked to each other, requiring a significant time commitment from officers accessing these systems. In its present state, the technology employed by SPD is not capable of meeting the needs of those tasked with reducing crime (Officer #1, 2011).

Further complicating matters is the reality that increasing the capabilities of any police force is very expensive. Funding for SPD for these expenses is received from the city of Salinas, which is in turn impacted by the weakness of the economy. With police

resources tied to both annual funding cycles and the economy, a recession provides gangs with increased opportunities to commit crime under the surveillance of a technologically challenged police force.

In 2010, the budget crisis in Salinas required the Chief of Police to reduce SPD by 19 sworn officers and 7 staff members to help balance the 2010/2011 budget (Fetherolf, 2010). In 2011, despite a 20% reduction in the city's workforce, a $7 million deficit remained resulting in the Mayor's announcement that additional vital services would be cut (Solana, 2011). According to Salinas Mayor Dennis J. Donohue, this deficit "will require some sacrifice by all city employees" (Solana, 2011). If citywide pay concessions are unable to close this gap, then SPD could face a 10% reduction in current funding. This would mean the additional loss of as many as twenty sworn and seven community service officers (Officer #3, personal communication, February 10, 2011). The above scenario paints a dire picture of SPD's ability to hold back the rising tide of crime and salvaging a sense of community from those who are attempting to tear it apart.

2. Capabilities

SPD also receives funding for resources through alternate sources such as state and federal grants. SPD has received the following capabilities via grant funding (T. Molfino, Personal Communications, January 26, 2011):

- Internet accessible digital voice recorders for use with field report writing (Funding source: Community Oriented Policing Service (COPS) Grant)
- 3G wireless Internet connectivity for all patrol vehicles mobile data terminals (MDT) including data plans for 18 months (Funding Source: Edward Byrne Memorial Justice Assistance grant program)
- 200 portable and 70 handheld vehicle mounted broadband radios as part of the NGEN Unity radio project (Funding source: COPS Grant)

While the above technologies will significantly improve SPD's immediate capabilities, they will also introduce significant challenges that, if not properly addressed, could reduce the long-term effectiveness of the force. Some of these technological challenges include:

- Integrating new technology into current business practices
- Adapting the culture of SPD to the new technologies being introduced
- Preventing unauthorized access and loss of sensitive information through the voice recorders and/or MDT
- Configuration challenges associated with integrating new technology into the existing information and communications architecture
- Compliance with local, state, and national data and information sharing standards

Responding to the above challenges creates a daunting task for any agency with a full time support staff and even more so for an agency that already had its manpower reduced and is looking at further reductions. Either way, these challenges must be addressed or SPD risks significant reductions in officer effectiveness.

Finally, gangs exhibit many similarities in "structure and tactics" to insurgent groups and exist "because of an information advantage bestowed upon them by the population" (Arnold, O'Gwin, & Vickers, 2010). This information advantage, when augmented with modern communications technology, such as smart phones, allows gangs to effectively coordinate and carry out acts of violence as demonstrated by the 2009 Salinas murder rate. Therefore, to combat gangs, the police need an information and communications architecture that goes beyond being able to respond to and apprehend the typically self-motivated but unorganized criminal such as a bank robber. The nightstick, flashlight, and side arm will not suffice to prevent or to reduce such crime. As long as the balance of information remains in favor of the gangs, the efforts of SPD will remain reactionary, as they will have no way to effectively respond to the organized yet unpredictable nature of gang violence (Lorentz, 2010). In its present state, the inefficiencies that exist in SPD's information and communications architecture create more opportunities for the criminals and reduce the tactical advantage for the SPD. This must change.

The above situation has severely hampered SPD in its ability to move forward in ways that will leverage the fight against crime in its favor. Of the potential solutions to these problems, the two most consequential towards SPD's crime fighting abilities are:

1. Acceptance: Continue with business as usual and wait for either better economic times or additional grant funding to support capability improvements, or
2. Adoption: Make better use of its existing Information and Communications capabilities in ways that enhance officer effectiveness.

This thesis focuses on the second option, and explains how aligning SPD's current capabilities to that of a JBAIIC-like architecture (discussed in Chapter I.B.1.) will help SPD reclaim the streets of Salinas from the deeply entrenched gang population.

B. FORMATION OF THE NPS/SPD WORKING GROUP

In December 2008, due to the increasing number of homicides in Salinas caused by a deeply rooted gang population, the Provost of the Naval Postgraduate School (NPS) requested that the NPS Defense Analysis (DA) Department provide assistance to the city of Salinas due to their expertise in irregular warfare (H. Rothstein, personal communication, September 21, 2010). Throughout the next year, representatives from the DA Department and the city of Salinas worked together to create courses of action to reduce gang violence. In August 2010, members of the NPS Department of Information Sciences joined the working group to aid in the fight against the rising crime in Salinas. From the Information Sciences Department, the Distributed Information Systems Experimentation Research Group (DISE) and its Intelligence Surveillance and Reconnaissance (ISR) field experimentation team, the Joint Battlespace Awareness ISR Integration Capability, (JBAIIC), formed a Technical Working Group (TWG) focused on identifying a viable, usable, and affordable solution to improve the Situational Awareness (SA) of the officers of the Salinas Police Department. According to JBAIIC's Project Team Leader,

> The [Technical] Working Group will be comprised of gang enforcement officers, field supervisors, communication (dispatch) professionals, and mid-level managers in addition to NPS personnel. The [technical] working group will provide input to NPS in accurately identifying a critical capability gap and that the proposed solution is operationally sound and would be reasonably likely to solve this gap. (B. Wood, personal communication, September 14, 2010)

1. JBAIIC—Joint Battlespace Awareness ISR Integration Capability

JBAIIC, is a field experimentation initiative that ensures, "ISR data collected—regardless of sensor, source or communications transport—is processed and exploited, making it available immediately to joint and coalition war fighters" (LeCappelain, 2010). The JBAIIC infrastructure consists of an experimentation lab located in Root Hall at NPS, three deployable trailers and one Mobile Command Post vehicle—the Joint Reconfigurable Vehicle (JRV). These assets allow the JBAIIC team to design, test, and overcome realistic battlefield ISR integration challenges that face deployed military units. The mobile trailers provide JBAIIC autonomous capabilities creating 'sensor to shooter' networks, allowing them to function as both a Tactical Operations Center (TOC) and Network Operations Center (NOC). As a result, JBAIIC is able to provide Command and Control[1] (C2) and Situational Awareness[2] (SA) for personnel at the TOC and those deployed to the tactical edge—the battlefield. With the ability to 'simulate' the entire information and communications process that exists on the battlefield, JBAIIC is uniquely able to test potential technologies to ensure they are able to provide the services needed by the military.

2. Initial Project Plan

After several meetings, the TWG identified the lack of a Common Tactical Picture (CTP)[3] as the most significant gap in SPD's architecture. To resolve this

[1] Command and Control (C2) is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (DOD Dictionary of Military Terms, 2011).

[2] Battlespace Awareness is the "knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission (DOD Dictionary of Military Terms, 2011). The term joint refers to those supporting partners such as coalition (foreign) or other U.S. service forces who are equally invested in the current action and therefore also need Situational Awareness.

[3] A Common Tactical Picture is "An accurate and complete display of relevant tactical data that integrates tactical information from the multi-tactical data link network, ground network, intelligence network, and sensor networks" (Common Tactical Picture, 2011). An Interactive Common Tactical Picture (I-CTP) is a CTP that is configured to accept user input.

deficiency, JBAIIC technicians tentatively planned two demonstrations to highlight how a Common Tactical Picture can enhance SA for SPD. The first demonstration, Demo #1, employed military technology to highlight a 'what is possible' while the second demonstration, Demo #2, would incorporate commercial technology to create a CTP that could be directly implemented by SPD. Table 1 shows the three phases of the project prior to Demo #1:

PHASE I
1. Analysis of current capabilities
2. Report project timeline
3. Establish a working group
a. Identify equipment for Demonstration # 1
b. Identify the equipment for Demonstration #2 (CTP Demo)
PHASE II
4. Demo #2 (CTP) for routine police operations
5. Demo #2 (CTP) for non routine operations
PHASE III
6. Solicitation for industry participation for Phase III technology capability demonstration
7. Host technology capability meeting to determine the exact range of sensor input possibilities for inclusion in the final demonstration
8. Final CTP Demonstration

Table 1. Project Plan (From B. Wood, personal communication, September 14, 2010)

a. Revised Project Plan

Shortly after completing the first demonstration, further analysis into SPD's architecture revealed that implementing a complete CTP was not in the best interest of SPD. There are many reasons for this. First, implementing Blue Force Tracking would require the NPS team to install either GPS or cellular devices on all patrol cars as well as configure the display on digital maps at the dispatch center. Due to two technological initiatives already in progress though, SPD would be able to implement BFT within the next year. Secondly, a CTP would need to be installed at the dispatch center to display the BFT position tracks. The dispatch center is not dedicated to SPD

alone, but instead supports every public safety agency in Monterey County. While technologically feasible, the efforts to properly integrate into this jointly used facility would need to consider the system impacts for all users, which is beyond the scope of this project. Finally, to display the position data, NPS would need to integrate this data into the the Computer Aided Dispatch (CAD) system at the dispatch center. However, this system is scheduled for replacement within three years. This means that any effort to integrate with the CAD would be short lived once the current system was replaced. With a police force still adjusting to recent reductions and several technological initiatives planned over the next year, SPD requested assistance with assessing its architecture as well as any recommendations for how to move forward from its present state. Researchers agreed with the modification listed in Table 2.

PHASE I
1. Analysis of current capabilities - Completed, Demo #1
2. Report project timeline - Completed, Demo #1
3. Establish a working group - Completed, Demo #1
a. Phase I - Identify the "equipment" for Demonstration # 1 - Completed, Demo #1
b. Phase I—Complete Demonstration #1 of CTP capability - Completed, Demo #1
PHASE II
4. Complete architectural analysis of SPD primary capabilities of a JBAIIC architecture
5. Identify capability gaps
PHASE III
6. Create a Technology Implementation Plan and Courses of Action

Table 2. Revised Project Plan

To accomplish this, researchers compare SPD's architecture to the architecture of JBAIIC and then provide recommendations to reduce capability gaps. Based on the results of this analysis and the technological initiatives already planned, a Technology Implementation Plan (TIP) would recommend potential courses of action for SPD in order to implement an architecture capable to combating the existing gang threat.

C. RESEARCH QUESTIONS

This thesis answers the following three questions:

- How can elements from the JBAIIC test bed knowledge base be adapted to the existing information architecture used by SPD to enhance its crime fighting strategies?
- How will members of SPD successfully implement the JBAIIC architecture?
- How could other municipal governments facing similar issues with high crime and constrained resources apply the architecture created for Salinas to extend the effectiveness of its police force?

1. Benefits of the Study

The implementation of an NPS-sponsored IT solution to real-life problems in a neighboring city will have a direct and beneficial impact on the citizens of Salinas and the Monterey Peninsula. The recent economic downturn and high crime rates have created an ideal time to leverage NPS research capabilities to implement IT measures that have already proven themselves overseas in the fight against deeply rooted insurgents employing irregular warfare tactics. After having identified the gaps in the existing information and communications architecture, NPS will be able to create a solid IT foundation on which to promote future research efforts. Finally, the methods used to employ a JBAIIC architecture for this research effort can be generalized and conveyed to other municipalities facing similar threats and resource constraints, allowing them to extend the capabilities of their limited resources.

2. Specific Research Objective

For the purposes of this study, the research objective is to use the JBAIIC architecture as a method to enhance the effectiveness of the capabilities of the Salinas Police Department. Specifically, given the current state of affairs in Salinas, the JBAIIC architecture model is used to identify both the capability gaps and those actions that the Salinas Police Department needs to take to achieve to prevent or attenuate the threats it currently faces.

II. METHODOLOGY

This research effort encompasses the alignment of the current architecture of SPD with that of a JBAIIC-like architecture to enhance officer effectiveness. To do this, the functional capabilities of SPD's architecture are compared to architectural elements of a JBAIIC architecture. Upon completion, any gaps identified from this analysis are incorporated into a Technology Implementation Plan (TIP) that recommends three courses of action considering the capability gaps as well as those IT initiatives currently in planned by SPD. This thesis encompasses a broad range of technologies but focuses only on those technologies that are believed to have the greatest impact on officer effectiveness. Due to the number of technologies being evaluated, this thesis does not delve into the specific technical issues surrounding the integration of any one technology, but instead focuses on how various technologies will impact the architecture of SPD to achieve Command and Control and Battlespace Awareness. The intent is that this thesis will be used as a strategic foundation of learning for SPD, allowing it to confidently and safely pursue enhancements to present capabilities, given its extensive resource limitations. The primary steps taken in the completion of this thesis include:

- Attending working group meetings between NPS and the city of Salinas
- Preparing for and participating in a Technology Demonstration in October 2010
- Assisting with the creation of information architecture drawings
- Documenting changes to the baseline JBAIIC architecture resulting in a best fit architecture for SPD
- Conducting a literature search for studies concerning various technology implementation initiatives in the Law Enforcement community
- Conducting interviews with members of SPD
- Performing inquiries with other California emergency service organizations that have implemented similar technologies for possible lessons learned and recommendations (e.g., biometrics, ShotSpotter, etc.).

A. JBAIIC'S INFORMATION AND COMMUNICATIONS ARCHITECTURE

The JBAIIC architectural model consists of six elements as identified in Figure 1. These elements, when integrated together, allow JBAIIC to obtain Command and Control and Battlespace Awareness as indicated by the green arrows pointing to the center. The following sections detail the explanations of each element.

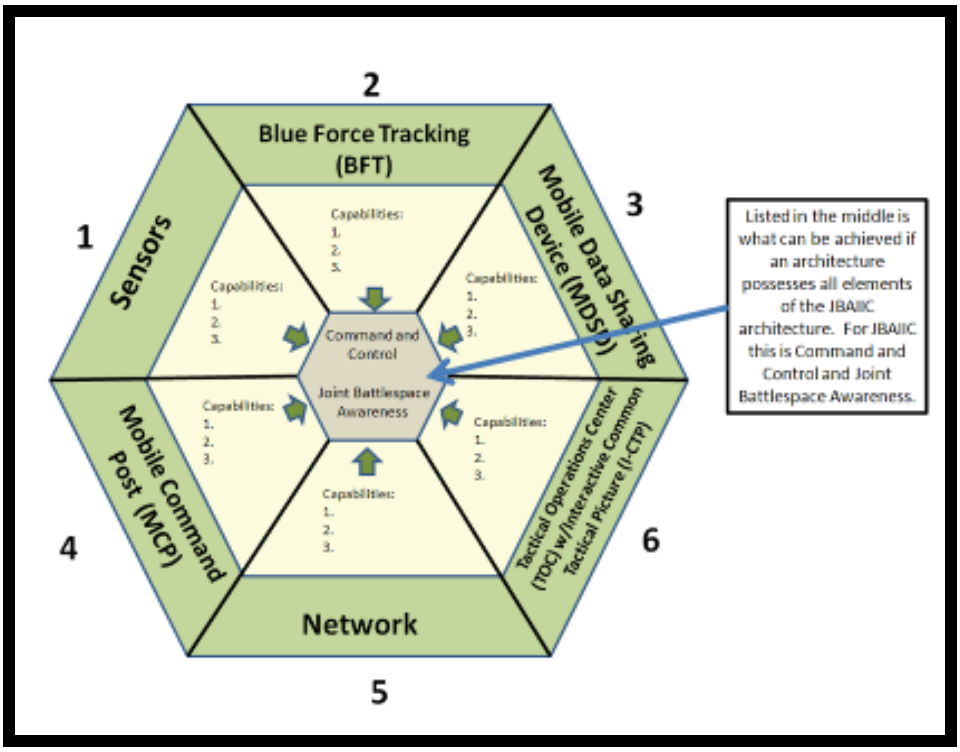


Figure 1. The JBAIIC Architectural Model

1. Sensors

Sensors are a key component of a JBAIIC-type architecture. Sensors of varying types are used to capture and relay information back to the Tactical Operations Center (TOC) for analysis and for inclusion in the Integrated Common Tactical Picture (I-CTP). Characteristics of a JBAIIC sensor include providing persistent sensing and adequate coverage of the battlespace. Examples of sensors used by JBAIIC to support recent research efforts include:

- Motion and Acoustic Sensors: Capable of locating movement, e.g., radars, such as Synthetic Aperture Radar (SAR), NanoSAR, Spotter RF radar, and ShotSpotter's Gunshot Location System (GLS).
- Optical Sensors: Detect thermal radiation or tacking pictures, e.g., Forward Looking Infrared Radar (FLIR)
- Seismic Sensors: Detect ground movement, e.g., Unattended Ground Sensors (UGS)
- UAS/UAV (Unmanned Aircraft System/Unmanned Aerial Vehicles): Mobile platforms capable of hosting a myriad of individual sensors, e.g., Predator and Scan Eagle drones.
- Aerostats: Moored balloons hosting a sensor platform

2. Blue Force Tracking

Blue Force Tracking (BFT) is a "United States military term used to denote a GPS-enabled system that provides military commanders and forces with location information" of friendly units ("BFT", 2011). BFT allows the Tactical Operations Center (TOC) to remain cognizant of deployed force locations including ground and air assets. Characteristics of BFT, as implemented by JBAIIC, include a GPS enabled device that is deployed on all assets and personnel. JBAIIC implements BFT by utilizing GPS enabled devices, such as tactical radios. The position data is then pushed to the TOC for display on an I-CTP.

3. Mobile Data Sharing Device (MDSD)

In the context of a JBAIIC architecture, Mobile Data Sharing Devices (MDSD) are ruggedized portable devices used to send, receive, and process information. Other characteristics of MDSDs are that they support both classified and unclassified data transfer, fully function in a bandwidth limited environment, and support data *push*,[4] *pull*[5]

[4] Data push commonly refers to a client server architecture in which data is "pushed" to a user's device rather than "pulled" by the user. In other words, the data transfer is initiated by the server rather than the client (Push, 2011). For the purposes of this report however, the meaning of Push indicates the ability to upload data to the network.

[5] Data pull is where data transfer is initiated by the client rather than the server. For the purposes of this report, the meaning of Pull indicates the ability to download data from the network.

and *sharing*.[6] Examples of MDSDs used by JBAIIC in both Empire Challenge 2009 and 2010 include: the Panasonic Toughbook (both CF-19 & CF-U1), Trimble's Nomad, General Dynamic's MR-1, SNC's Tacticomp T1.5 & T5, and the handheld Lockheed Martin Distributed Operations (DisOPS). These devices can be used to support numerous operational needs such as mission planning, Chat, VOIP (Voice Over Internet Protocol) communications, BFT monitoring, viewing maps, capturing and forwarding video, and providing simultaneous access to the CTP. Depending on the experiment, MDSDs may be used in either a fixed, mounted, and/or dismounted capacity and will need to be capable of line-of-sight or satellite communications, or both. This allows both deployed forces and the TOC to remain cognizant of nearby threats, reducing the response time to enemy actions.

4. Mobile Command Post

For deployed forces without direct satellite communications, there needs to be a means of getting data to and from the TOC and between other forces over the horizon. This is the job of the Mobile Command Post (MCP). A MCP is a deployable mobile platform that has more robust communications and information systems than those of the deployed forces. An MCP must be able to support both classified and unclassified data traffic, have the ability to communicate directly with the TOC, and possess redundant communications capabilities. An MCP extends the viewable battlespace by providing a means for the deployed forces with reduced communications capabilities, to relay information to the TOC. The MCP acts as a sensor point of entry and provides an interface to numerous networks. With a direct connection to the TOC, an MCP allows deployed forces to access more of the battlespace further enhancing Situational Awareness (SA). Figure 2 shows JBAIIC's MCP called the Joint Reconfigurable Vehicle (JRV).

[6] Information sharing is synonymous with "peer to peer," which means that computers are able to share data directly between themselves without the use of a server. The term "share" is used here because the author believes it more easily communicates an essential need of a JBAIIC architecture concerning MDSDs.

Figure 2. JBAIIC's Mobile Command Post the Joint Reconfigurable Vehicle (JRV) USJFCOM photo by Staff Sgt. Vanessa Valentin, USAF

5. Network

The network component of the JBAIIC architecture is composed of the data paths that connect the sensor network to the MDSDs, MCPs, and TOC in addition to external communities of interest. Successfully resolving these *one to many - many to one* networking challenges is very complicated and is what makes JBAIIC so unique among military IT integration platforms. To fulfill its mission as an autonomous Intelligence, Surveillance, and Reconnaissance (ISR) test bed, a JBAIIC architecture usually consists of numerous classified and unclassified networks. These networks, or enclaves, are configured to allow *low* to *high* cross-domain data sharing of everything from chat communications, sensor data, to CTP data. Figure 3 shows an example of a JBAIIC network created to provide a Secure Network Server,[7] Cross Domain Solution as part of Empire Challenge[8] 2009 (EC, 2009). Table 3 lists the security domains that supported EC 2009.

[7] Secure Network Server (SNS) is a Cross Domain Solution developed by Boeing that supports bidirectional data sharing among multiple security enclaves (Irvine, 2009).

[8] Empire Challenge is an annual U.S. Joint Forces Command (USJFCOM) led multinational ISR demonstration that showcases emerging capabilities and provides lessons learned to improve joint and combined ISR interoperability (LeCappelain, 2010).

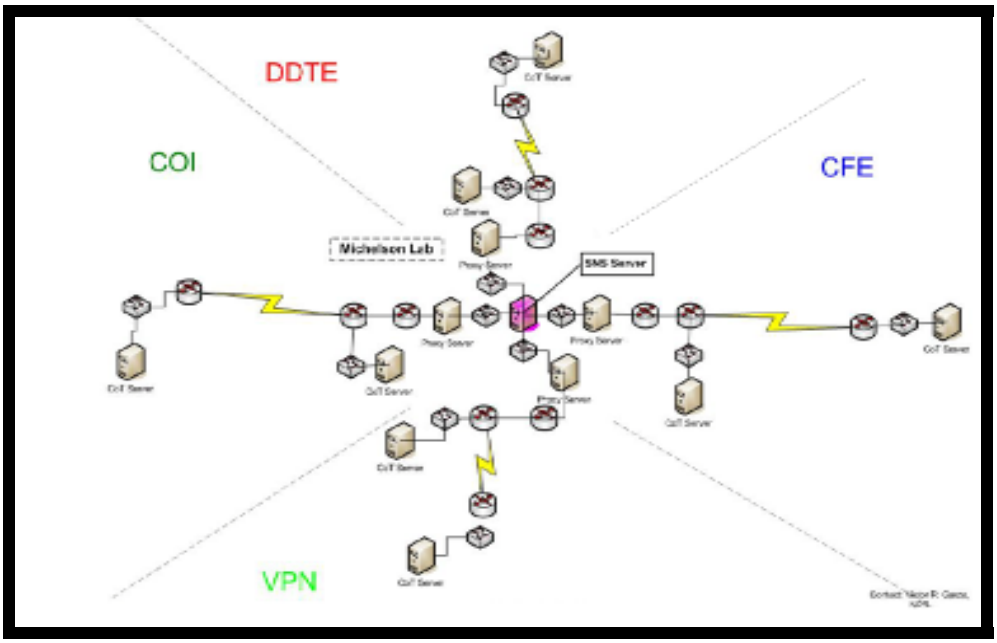


Figure 3. JBAIIC Architecture for Secure Network Server, Cross Domain Solution as Part of Empire Challenge 2009 (From Garza, 2009)

Security Domains Supported by SNS in EC09	
Security Domain	**Classification Level**
Virtual Private Network (VPN)	Unclassified
Community Of Interest (COI)	Unclassified
Coalition Four Eyes (CFE)	Secret, Coalition
Distributed Development and Test Enterprise (DDTE)	Secret, U.S. only

Table 3. Security Domains as Part of Secure Network Server, Cross Domain Solution

In addition to configuring the physical devices that host the network, the JBAIIC team has to integrate the communications links connecting tactical devices. Elements commonly incorporated into a JBAIIC network for field experimentation include a tactical satellite and secure wireless, typically UHF, VHF, or commercial 3G/4G cellular. The proper configuration of a JBAIIC network is essential for testing emerging ISR capabilities.

6. Tactical Operations Center (TOC) and Interactive—Common Tactical Picture (I-CTP)

The Tactical Operations Center (TOC) is the 'brains' of any modern warfighting effort. At the TOC, sensor and intelligence data are fused together to create an I-CTP which provides battlespace awareness that operational commanders need to exercise C2 over their forces. Once created, the CTP can then be pushed to tactical units deployed throughout the battlespace for display at either Mobile Command Posts or on individual Mobile Data Sharing Devices. Essential characteristics of a JBAIIC TOC include:

- The ability to receive classified and unclassified sensor data,
- Hosts a CTP available to both internal and external users, and
- Employs analysts who are focused on synthesizing sensor data to create actionable intelligence.

To create the CTP, JBAIIC uses the MITRE Cursor on Target (CoT)[9] technology. "CoT translates metadata from ISR systems and sensors into a common message format for display on the CTP. The images received at the TOC are embedded in CoT messages. These image messages are normally displayed as camera icons on the FalconView CTP display. The user can access these images by clicking on the icon" (Irvine, 2011). Being able to access the location of friendly and enemy forces on a CTP greatly enhances the SA of the community of users.

As an autonomous ISR integration test bed, JBAIIC is specifically equipped to perform the duties of the TOC. To fulfill this role, JBAIIC utilizes three mobile platforms: Joint Mission Support Modules #1 (JMSM-1), #2 (JMSM-2), and #3 (JMSM-3). JMSM-1 functions as a Network Operations Center (NOC); JMSM-2 provides the C2 displays for SA and fulfills the role of TOC; and JMSM-3 is a workshop that supports both JMSM-1 and JMSM-2. Figure 4 shows the interior of the JBAIIC TOC (JMSM-2) and Figure 5 displays how TOC and CTP integrate within the JBAIIC infrastructure.

[9] CoT is a "MITRE-developed XML methodology for communicating essential battlefield information (where, when, and what) between otherwise non interoperable systems and is the mechanism employed by JBAIIC for ISR integration (Irvine, 2009)."

Figure 4. Interior of the JMSM-2 TOC on August 12, 2010. Photo by JBAIIC (From Irvine, 2009)

Table 4 summarizes the characteristics of a JBAIIC architecture. These characteristics were used to determine how SPD's architecture compares to JBAIIC's architecture. Following Table 4, Figure 5 provides an overview of the JBAIIC Infrastructure as detailed in the previous pages.

JBAIIC Architecture	Characteristics of the JBAIIC Architecture Elements[10]
Sensors	1. Sensors provide persistent monitoring of battlespace 2. Enough sensors are deployed to cover the battlespace
Blue Force Tracking (BFT)	1. Implemented with GPS 2. Deployed on all assets and personnel
Mobile Data Sharing Devices (MDSD)	1. Must support both classified and unclassified transfer of data 2. Supports 'Push, Pull, & Share' of data (as defined in section II) 3. Fully functions in bandwidth limited environment 4. Ruggedized design
Mobile Command Post (MCP)	1. Must support both classified and unclassified transfer of data 2. Direct communications with local units and Tactical Operations Center (TOC) 3. Redundant communications 4. Must be fully operational
Network	1. Support classified and unclassified communications: a. audio, b. video, and c. data 2. Must be able to communicate with coalition partners
Tactical Operations Center (TOC) with Interactive Common Tactical Picture (I-CTP)	1. Able to receive classified and unclassified data from sensor network 2. Receives input from all elements of the JBAIIC architecture 3. Displayable for local and external uses 4. Full time analysts who fuse sensor data into actionable intelligence

Table 4. Summary of JBAIIC Architectural Characteristics

[10] For the purposes of this study, the requirement of JBAIIC architecture elements to support classified and unclassified data will be deemed to be met by SPD capabilities able to support secure (encryption) and non-secure modes of data transport.

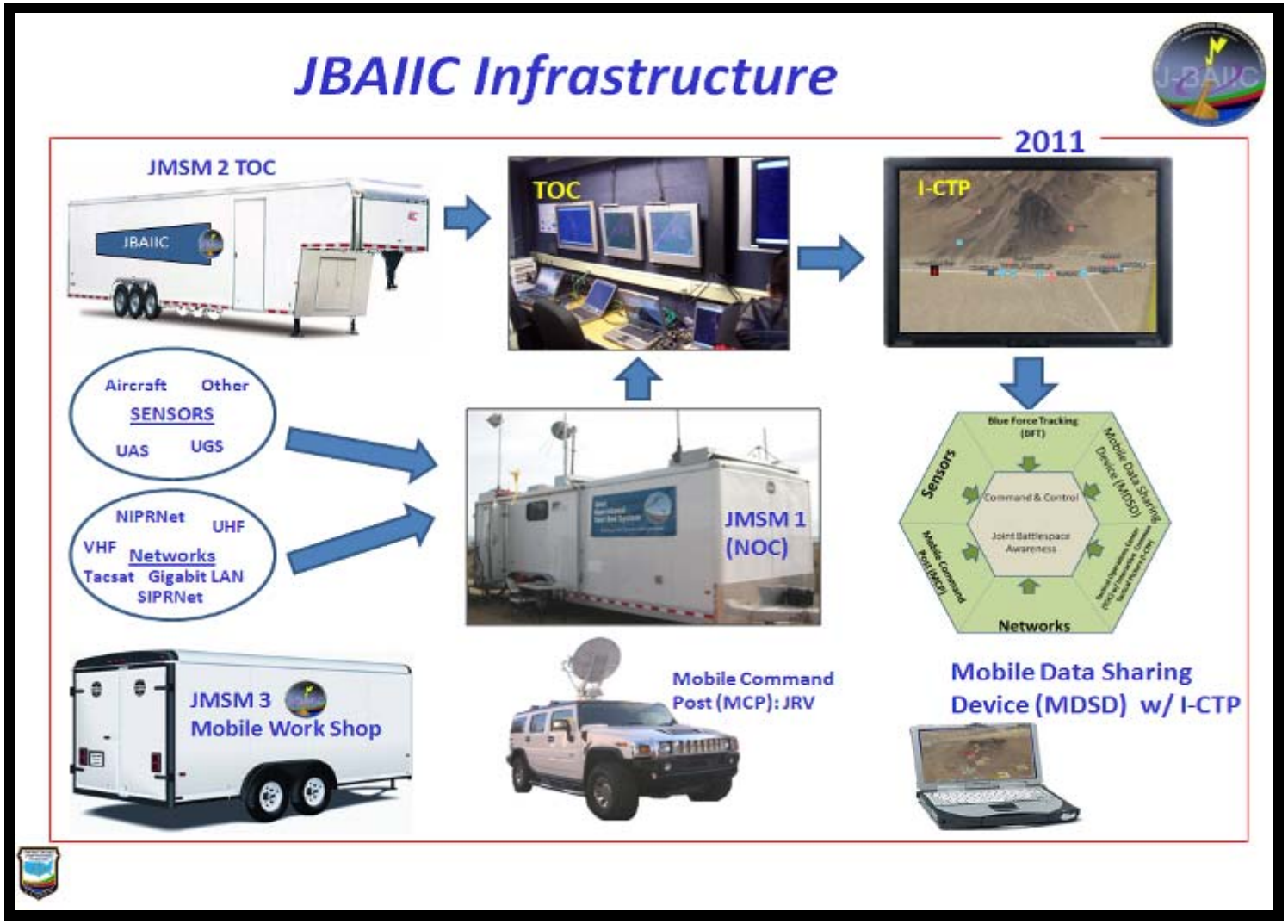


Figure 5. JBAIIC Infrastructure

In addition to possessing the six elements identified in the JBAIIC model, each element must be integrated with the others. It is through the integration of these elements that ultimately results in a JBAIIC architecture capable of providing Command and Control and Battlespace Awareness at both the TOC and among the deployed field units. For the purposes of this study, assessing the level of integration of SPD's architecture includes only a relative determination of the overall architecture's ability to access data as it relates to a JBAIIC architecture. The terms *push*, *pull*, and *share* are used to demonstrate a relative level of overall system integration. Figure 6 displays the author's interpretation of three types of system integration, which include *Non Integrated*, *Partially Integrated,* and *Fully Integrated Systems*.

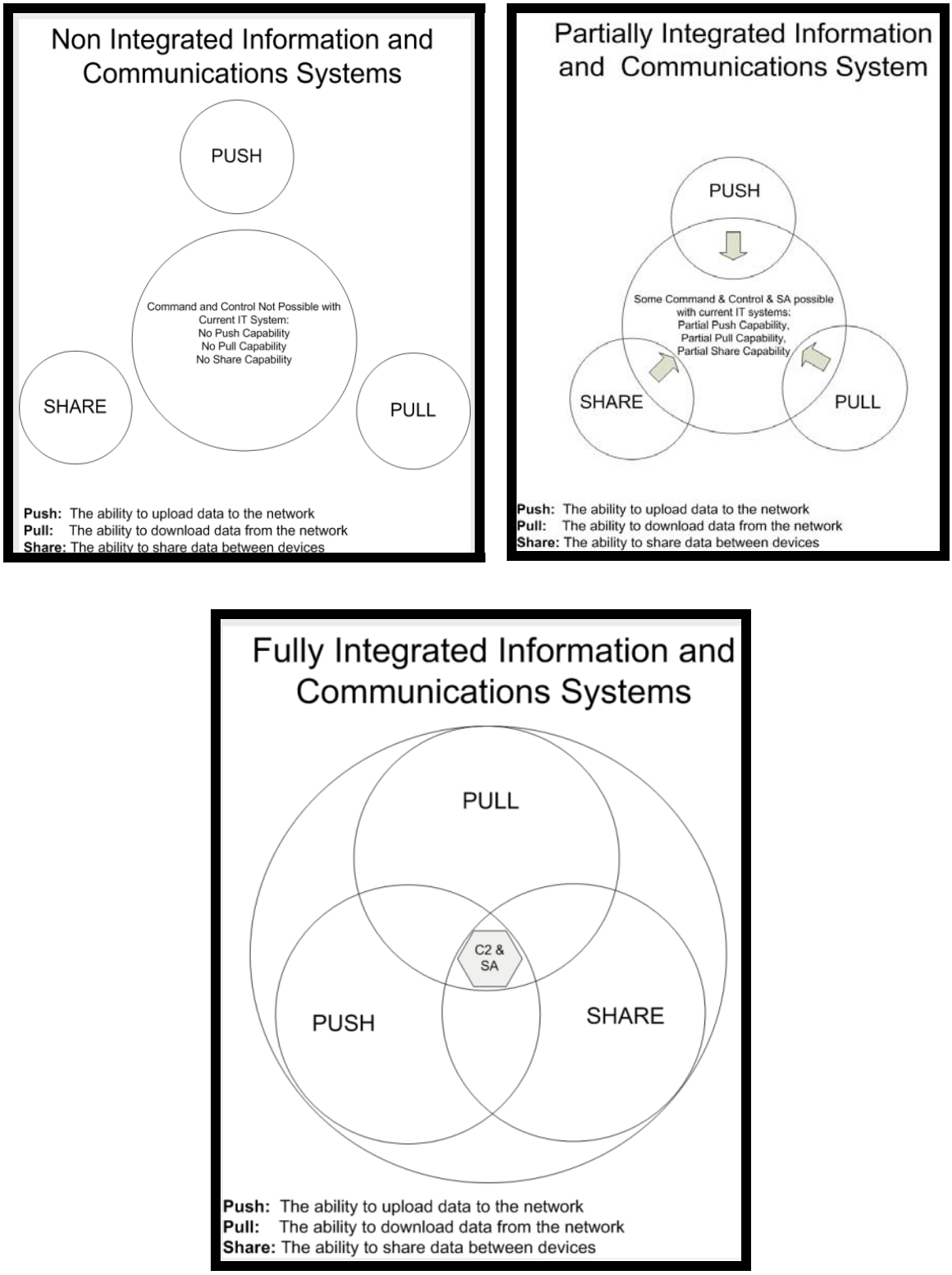


Figure 6. Venn Diagram Identifying Relative Levels of IT System Integration Non Integrated, Partially Integrated, and Fully Integrated

Together, the architectural model (Figure 1) and those capabilities listed in Table 4 make up the baseline JBAIIC architecture, which was used to assess SPD's architectural capabilities. By comparing its capabilities to that of the JBAIIC architecture, SPD will be able to identify those capability gaps that are limiting its ability to achieve Command and Control and Battlespace Awareness on the streets of Salinas. Once identified, SPD will be able to create a plan of action allowing them to achieve the benefits of the JBAIIC architecture which include the ability to "access, aggregate, disseminate, and display key information at the tactical edge to provide improved situational awareness and facilitate more effective decisions" (Irvine, 2009).

B. JBAIIC'S ARCHITECTURE FOR SEAL TEAM EIGHT

To ensure SPD's architecture is able to combat violent crime, it must be aligned with an architecture best suited for that purpose. The JBAIIC information and communication architecture (from now on referred to as the 'JBAIIC architecture') is such an architecture.

A JBAIIC architecture was recently created for Seal Team EIGHT to support wartime operations. Figure 7 shows how an architectural model can be used to combat a specific threat. Specifically, in the case of Seal Team EIGHT, the architectural model organizes the capabilities to combat insurgents.

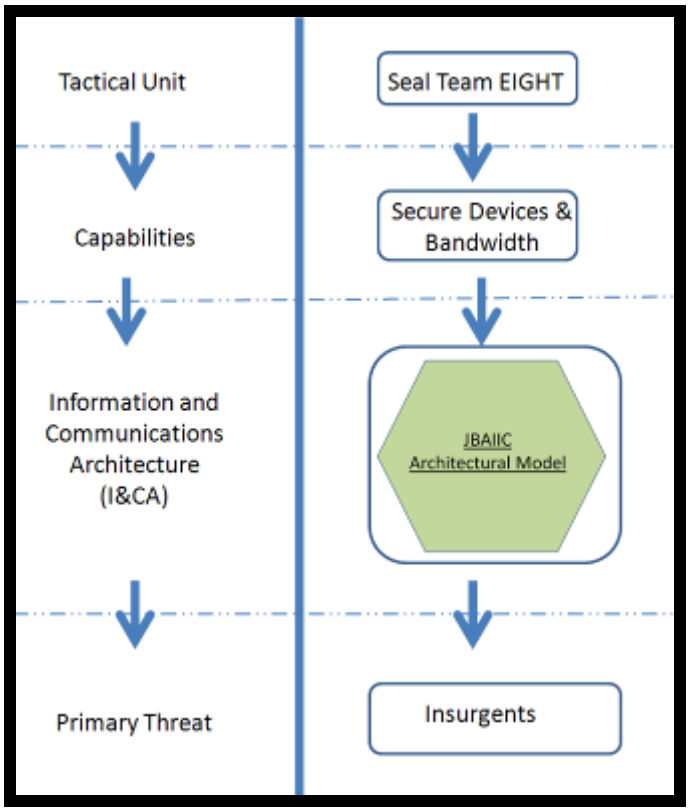


Figure 7. How an Architectural Model Is Used to Address Threats.

Figures 8 and 9 show two different views of a JBAIIC architecture created to support Seal Team EIGHT. Figure 8 demonstrates how tactical units using secure radios can relay real time information to a TOC via an MCP for use in creating I-CTP to achieve Battlespace Awareness.

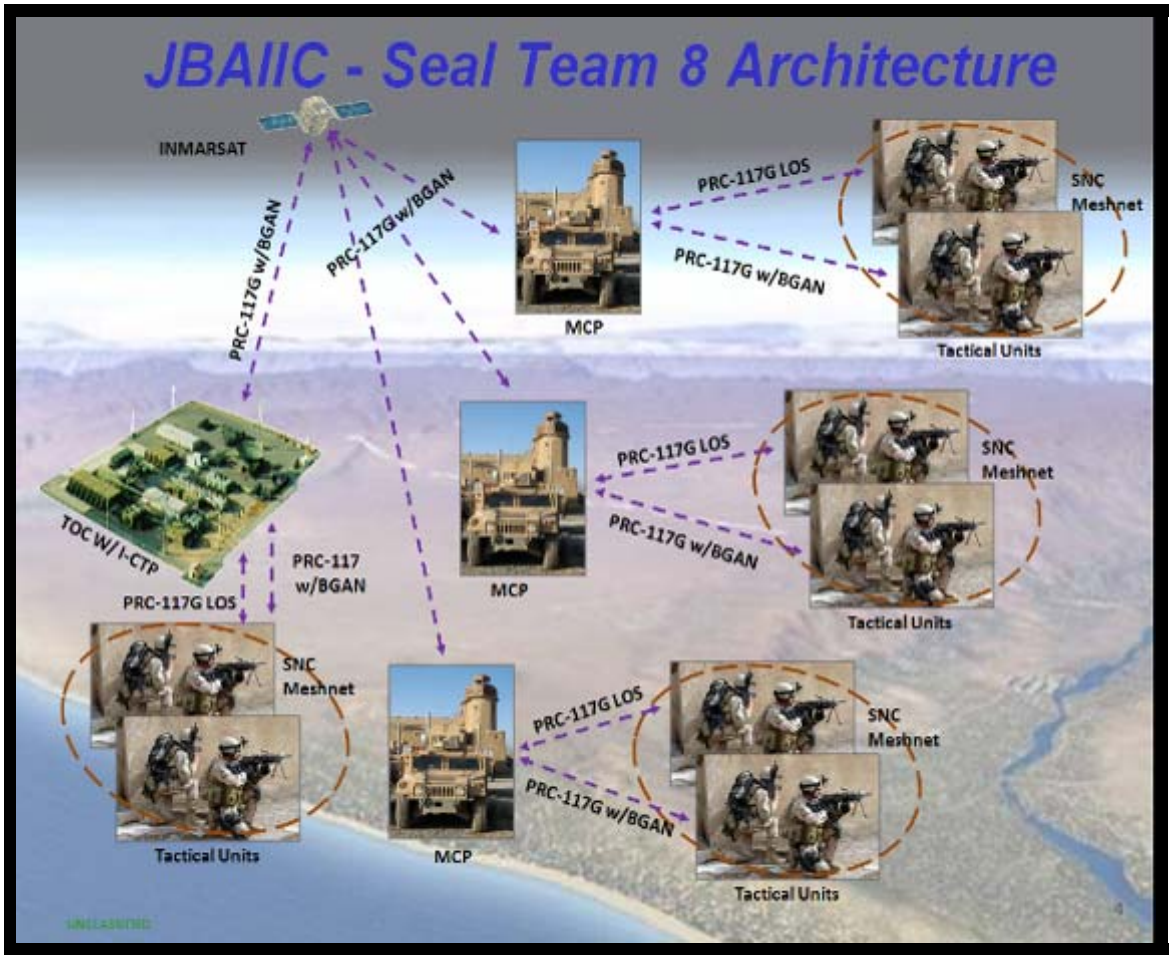


Figure 8. JBAIIC Architecture View #1—Seal Team EIGHT (From Roeting, 2010)

Figure 8 Acronyms	
BGAN: Broadband Global Area Network (e.g., INMARSAT Service) **INMARSAT**: International Maritime Satellite Communications **LOS**: Line-of-sight **MCP**: Mobile Command Post **MDSD**: Mobile Data Sharing Device **PRC-152**: Tactical Radio made by Harris Radio **PRC-117G**: Tactical Radio made by Harris Radio **SNC Meshnet**: A "fault-tolerant high-performance local area network" that utilizes SNC communications devices (Kulkarni, Malaiya, & Jayasumana, 1989).	**SNC T5.0** Tactical Tablet Mobile Data Sharing Devices (MDSD) made by SNC **SNC T1.5**: Tactical Handheld Mobile Data Sharing Devices (MDSD) made by SNC **SNC**: Sierra Nevada Corporation **TOC w/ I-CTP**: Tactical Operations Center with Interactive Common Tactical Picture

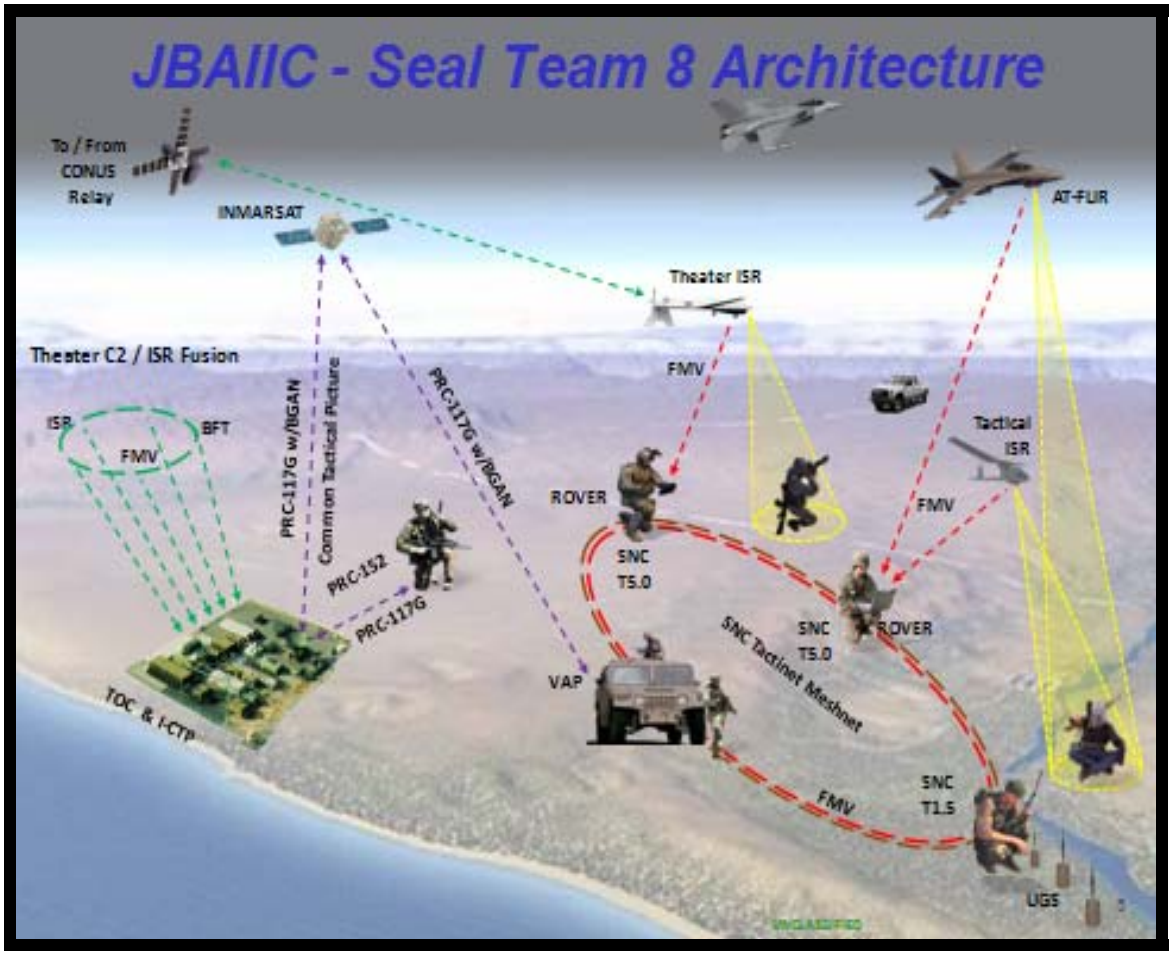


Figure 9. JBAIIC Architecture View #2—Seal Team EIGHT (From Roeting, 2010)

Figure 9 Acronyms	
AT-FLIR (Advanced Targeting—Forward Looking Infrared Radar): An aircraft mounted radar sensor made by Raytheon **BFT**: Blue Force Tracker **FMV**: Full Motion Video **ISR**: Intelligence, Surveillance, and Reconnaissance	**Rover**: Remotely Operated Video Enhanced Receiver **Tactical ISR**: A deployable ISR sensor **UGS**: Unattended Ground Sensor **VAP**: Virtual Access Point—A wireless devices that provides network access to deployed forces

Figure 9 shows how sensors can be integrated into this architecture, enabling real-time information sharing between deployed forces equipped with Mobile Data Sharing Devices (MDSD) and the TOC. The yellow cones originating from the airborne sensors (AT-FLIR) identify hostile targets. This data is relayed to ground forces and displayed

on MDSDs such as the Sierra Nevada Corporation's (SNC) T5 tablet or T1.5 handheld device. These figures demonstrate the power behind a fully integrated JBAIIC architecture. Once implemented, this architecture allowed Seal Team EIGHT to achieve 'sensor to shooter' decision timelines for both the tactical units and the TOC.

Figure 10 shows the final JBAIIC architecture created for Seal Team EIGHT. For assessment purposes, green check marks were used to indicate that a given capability does contribute to the architectures overall ability to achieve C2 and SA. Red Xs indicate that a given capability does not contribute to the architectures overall ability to achieve C2 and SA and constitutes a capability gap. Those capabilities listed in the off-white center section are those most critical to achieving the characteristics of a JBAIIC architecture. By aligning its capabilities to that of the JBAIIC baseline architecture, Seal Team EIGHT is able to achieve both Command and Control and Joint Battlespace Awareness.

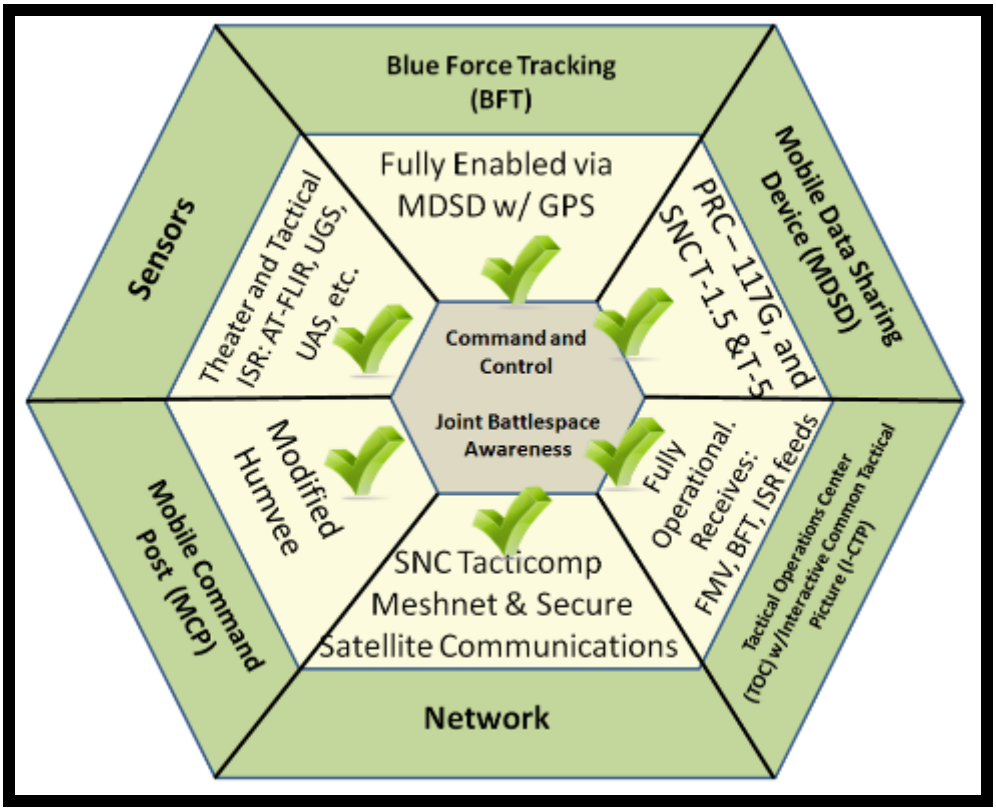


Figure 10. JBAIIC Architecture for Seal Team EIGHT

C. SPD-JBAIIC ARCHITECTURE - DEMONSTRATION #1

1. Concept and Setup

To demonstrate how a JBAIIC architecture can result in both improved command and control and battlespace awareness, researchers from the Naval Postgraduate School conducted a field demonstration for SPD on October 14, 2010, in Salinas, California. By using GPS-enabled Mobile Data Sharing Devices, researchers demonstrated the advantage of being able to observe officer locations via Blue Force Tracking, on a CTP during the response to two scenario-based events in different locations. Researches initially selected SPD's headquarters, Figure 11(a), and the dispatch center, Figure 11(b), as the locations for the demonstrations. Upon the completion of site surveys researchers created a preliminary network diagram (Figure 12).

(a). Dispatch Center Aerial View

(b). Salinas Police Department Aerial View

Figure 11. Proposed Sites for JBAIC's Field Demonstration

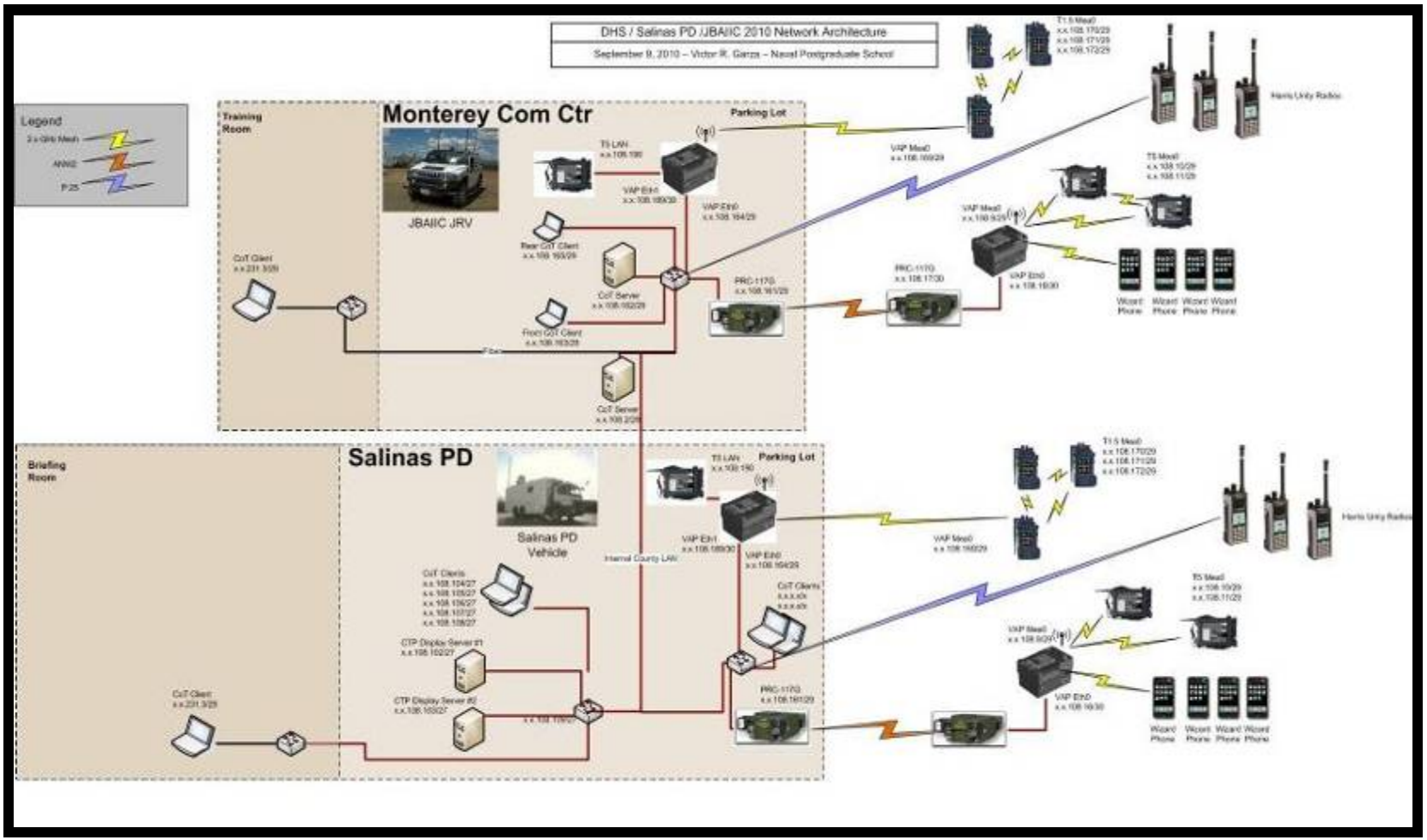


Figure 12. Initial JBAIIC Network Architecture for Demonstration #1 Diagram created by Bob Garza, JBAIIC

Prior to the demonstration, the dispatch center became unavailable to stage the experiment. This required shifting this portion of the demonstration to the Salinas Fire Department (SFD) Abbott Street Fire Station (Figure 13). The TOC was set up in the fire station training room and the Mobile Command Vehicle (MCV), acting as an MCP, was deployed across the street from SPD headquarters. To connect the MCP to the TOC, researchers erected a 65-foot omni-directional antenna connected to a Harris PRC-117G tactical radio at each site to provide a line-of-sight communications link. Due to the change in venue researchers adjusted the network diagram to accommodate the change in location (Figure 14). At the TOC, two CTPs displayed the outputs of the MDSDs, allowing SPD observers in the TOC to view both scenarios. Furthermore, officers participating in the scenario would be able to monitor the situation from a CTP being pushed to their handheld devices from the TOC. Researchers crafted two scenarios (conducted twice each) for the demonstration. Prior to the start of each scenario, participating officers were each issued a GPS-enabled SNC handheld device so that officer locations could be displayed on the CTP at the TOC.

a. Scenario #1

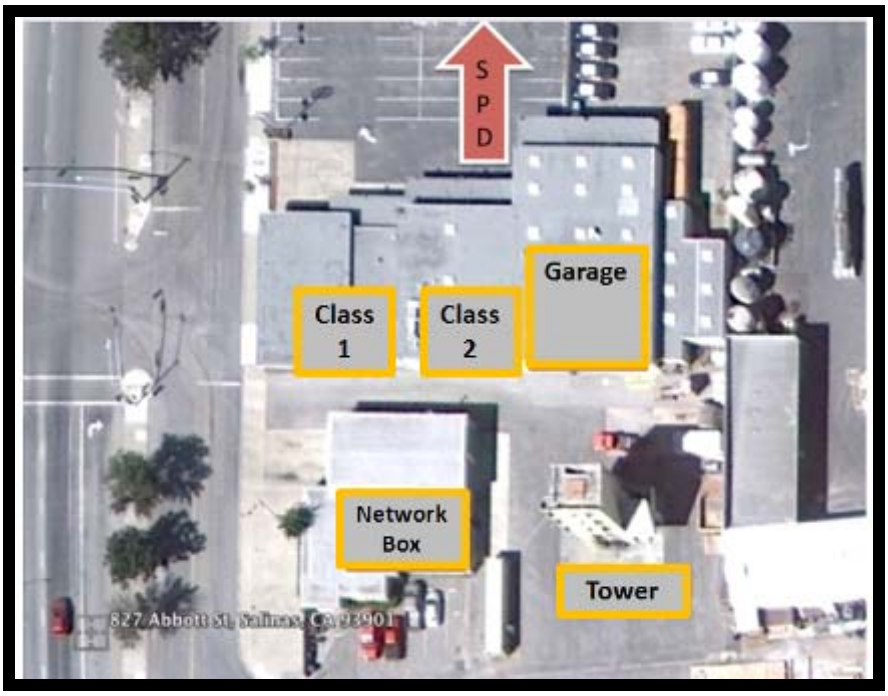
The first scenario took place in a parking lot at SPD Headquarters. It involved officers responding to a report of a suspicious person. A researcher acting as a bystander observed a suspicious person, and simulated calling 911 by briefing real dispatchers participating in the scenario. Upon receiving the 911 call, the dispatcher sent a participating officer to the scene. Once on scene, the officer requested backup. Once backup arrived, both officers approached the suspicious person. The primary officer placed the individual under arrest and escorted him to the rear of SPD. The scenario was then repeated.

b. Scenario #2

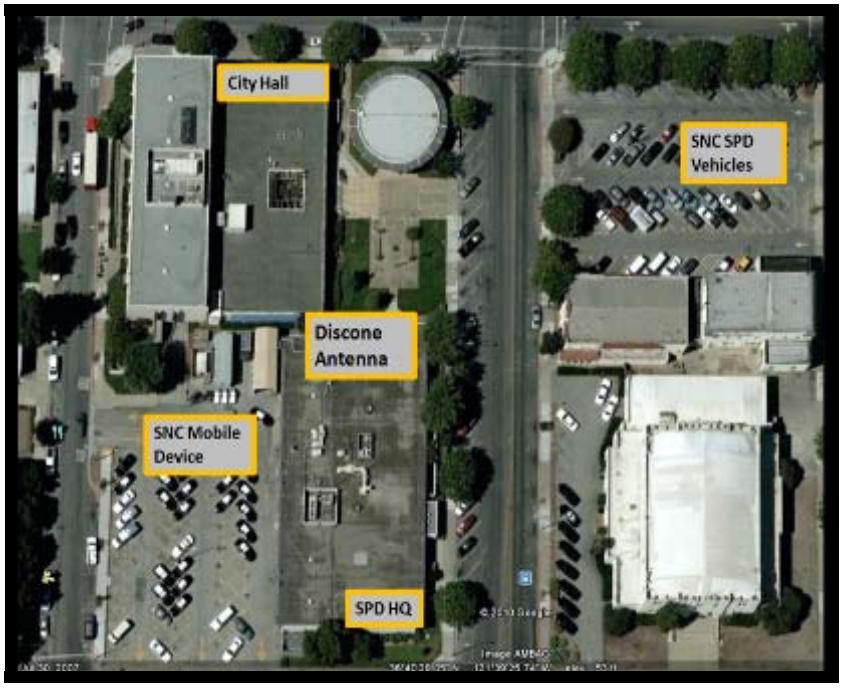
The second scenario occurred simultaneously with Scenario #1, but across town at the Abbott Street Fire Station. This scenario involved a simulated drive-by shooting. In this scenario, an armed assailant shot a person but then remained in the area for an unknown reason. An observer reported the incident to the dispatch center. Two

SPD units, each with BFT enabled mobile devices, and an ambulance (simulated) were dispatched to the scene. Once on scene, the officers took the suspicious person into custody. The victim, seeing that he was only shot in the foot, refused medical assistance and was escorted back to the Fire Station training room, concluding the scenario. All participants in Scenario #2 gathered in the SFD training room for a debriefing. The participants then repeated the scenario.

After both scenarios were completed twice, researchers conducted a mass debriefing inside the TOC at SFD. Here, data collectors interviewed scenario participants about their experience with the Mobile Data Sharing Devices, and asked whether implementing Blue Force Tracking could assist officers in the performance of their duties.



(a). Salinas Fire Department, Aerial View



(b). Salinas Police Department, Aerial View

Figure 13. Site Locations for JBAIIC's Field Demonstration

2. Final Architecture and Challenges

Throughout the preparation and execution of this effort, many challenges and lessons were learned. Prior to the demonstration, the most significant challenge involved coordinating the participation and resource use of both the city of Salinas and Monterey County public safety agencies resulting in significant changes to the initial network architecture (Figure 12) and the final network architecture (Figure 14). For example, the change in location, from the dispatch center to SFD, significantly impacted the network and communication aspects of the demonstration. The roof of the dispatch center provided an optimal height that enabled the communications antennas to connect to the Mobile Data Sharing Devices distributed throughout the two site locations. At the Fire Station, the tower used to mount the antennas provided a lower antenna height, which resulted in intermittent communications throughout the event.

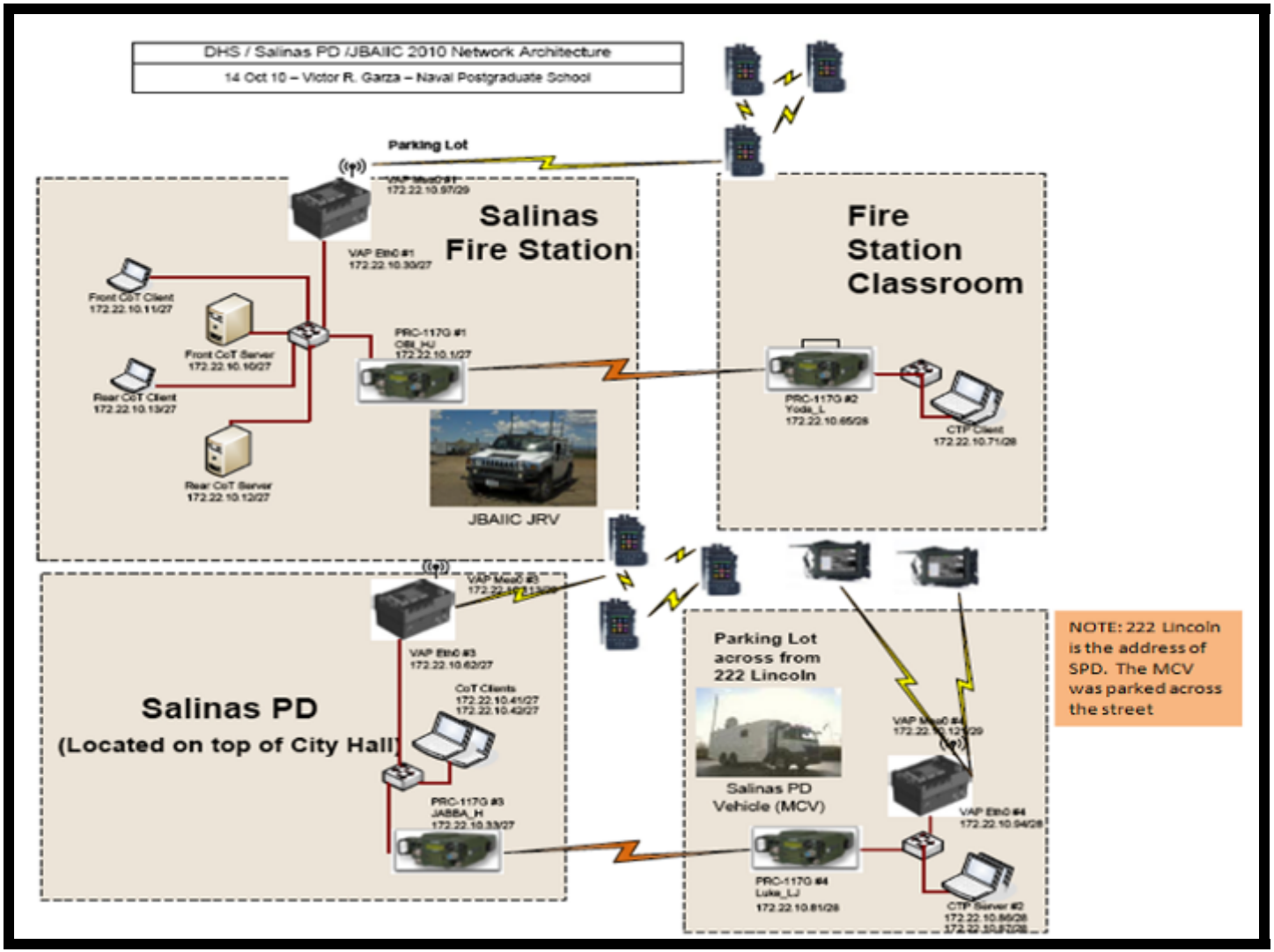


Figure 14. Final JBAIIC Network Architecture Demonstration #1 (Diagram created by Bob Garza, JBAIIC)

Of the many challenges that surfaced during the demonstration, the two most significant ones were:

- maintaining adequate signal strength between the two PRC-117G radios at SPD and SFD sites, and
- resolving the significant delays (up to 10 seconds) in the refresh rates of the icons that identified the location of the officers. This resulted in the CTP 'lagging' behind the actual events as heard on the radios.

We believe that the poor signal strength and long refresh rates were the result of:

- the maximum available height of each antenna resulting in a less than optimum line-of-sight between the two nodes,
- urban interference caused by the surrounding buildings, and
- environmental interference caused by strong winds and warm local temperatures.

3. Results of Demonstration #1

Despite the challenges, SPD officers involved in the scenarios were able to observe how BFT, when implemented into a CTP, provides enhanced SA to those at the TOC. For example, one officer stated that a CTP with BFT would not only be advantageous to local officers but would be essential for providing SA to officers who are responding from other jurisdictions—such as the County Sheriff's Department—who may not be familiar with the local area (Officer #5, personal communication, October 14, 2010).

Figure 15 is the JBAIIC Architectural model created for this demonstration. It identifies which capabilities of SPD, SFD, and JBAIIC team result in achieving C2 and Battlespace Awareness.

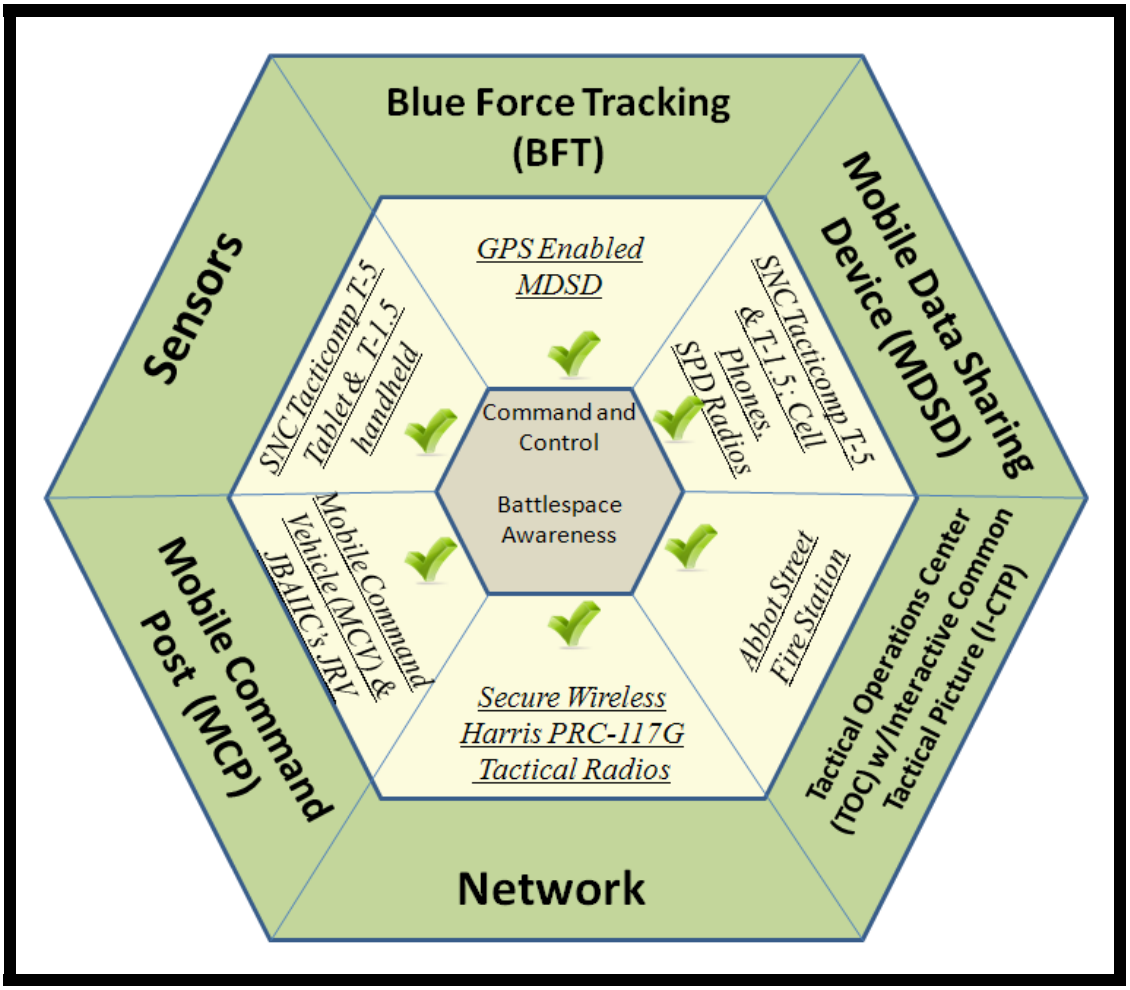


Figure 15. Final JBAIIC Architecture Model, Demonstration #1

While effective, the model in Figure 15 is not a practical solution for SPD because the military tactical radios are cost prohibitive and not ubiquitous among SPD partner agencies throughout Monterey County. To create a Salinas-specific JBAIIC architecture, the author completed an analysis of the current architecture of both SPD and a typical street gang. By doing this, the author was able to create a JBAIIC-type architecture that can exceed the capabilities of the violent criminals in Salinas.

D. SALINAS, CALIFORNIA, AND THE SALINAS POLICE DEPARTMENT

1. Salinas, California

Salinas, California, is located approximately 10 miles northeast of Monterey, California, and 100 miles south of San Francisco (Figure 16). The city is an agricultural center, 23 square miles in size, and produces nearly 80 percent of the lettuce in the U.S. ("Salinas California", 2011). The 2009 population of Salinas was 152,597, composed of 70 percent Hispanic, 18 percent White, 2 percent Asian, 1 percent African American, and 9 percent other (Long, 2010).

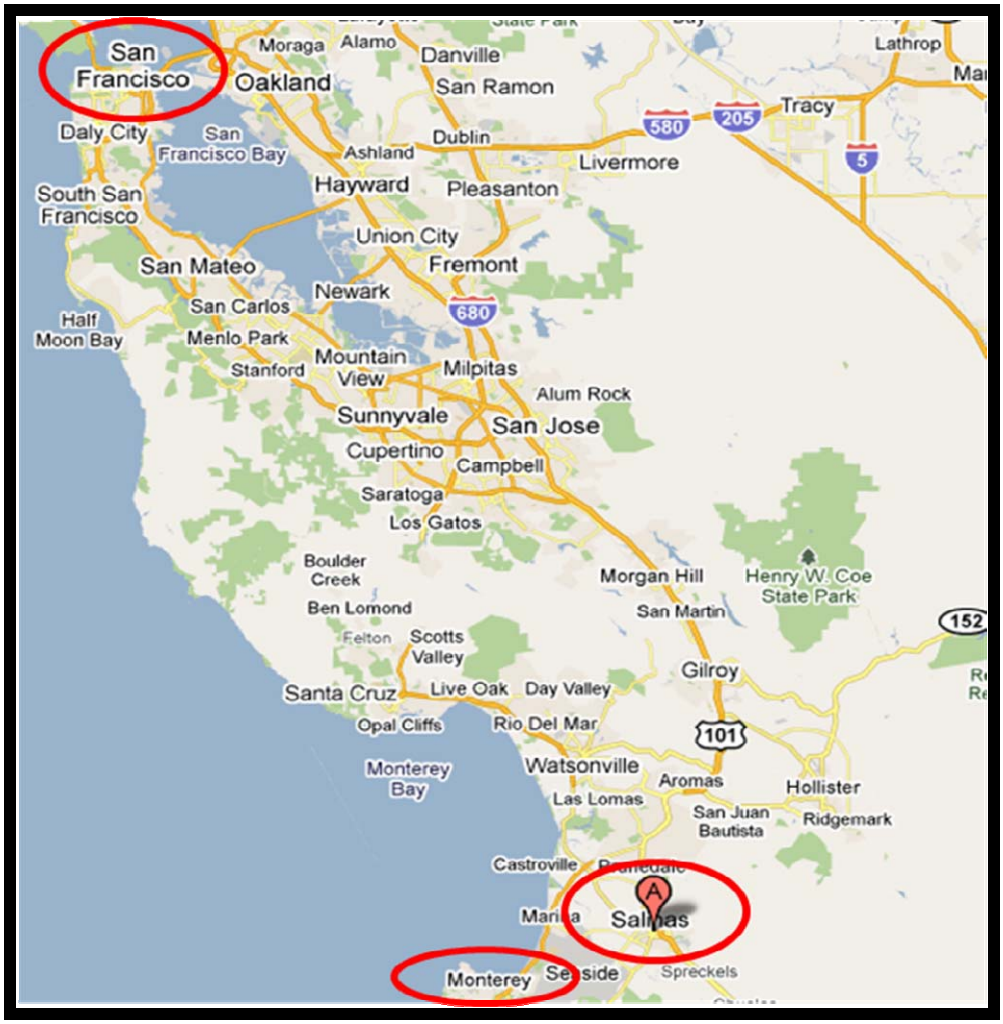


Figure 16. Salinas, California

2. The Salinas Police Department

The Salinas Police Department (SPD) is headquartered at 222 Lincoln Avenue (just off of Main Street) in historic downtown Salinas. As of February 18, 2011, SPD had 156 sworn officers, 59 full time and 15 part time staff, 13 reserve officers, and 16 volunteers. Excluding the executive staff, these personnel are distributed into three divisions: Investigations, Police Services, and Field Operations as shown in Figure 17.

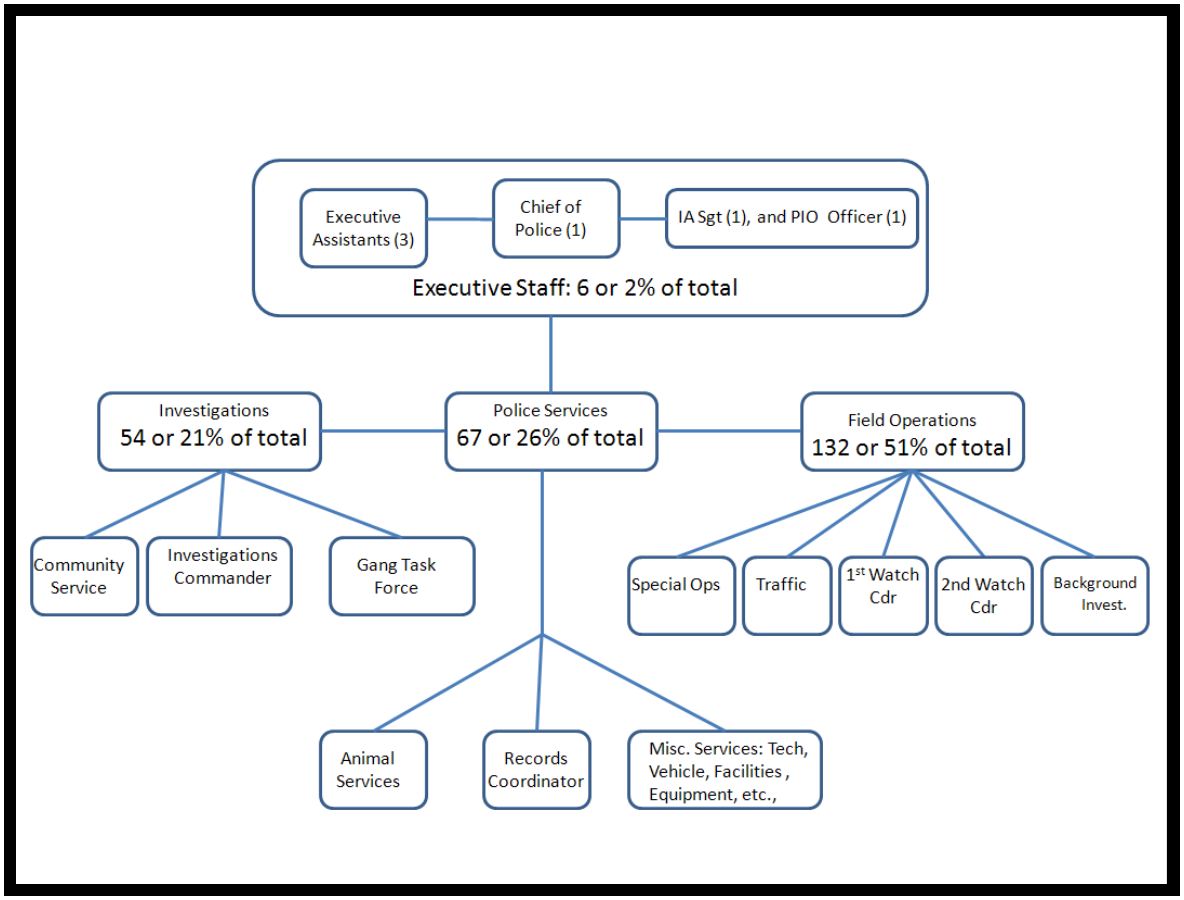


Figure 17. Formal Organization of SPD

SPD's organizational structure allows it to respond to the various needs associated with maintaining the peace in Salinas. To provide the services associated with public safety, SPD relies on a core set of tools, equipment, and technology to assist all officers in the performance of their duties.

In a typical day, officers, especially patrol officers, use the following equipment:[11]

- Patrol Car with vehicle-mounted mobile data terminal (MDT)
- Radio that is vehicle mounted and portable
- Magnetic Voice Recorders
- Cell Phones[12]
- Field interview forms and various other paper forms
- Standard issue police gear (personal weapon, handcuffs, note pad, body armor, etc.)

3. Patrol Operations

The Field Operations Division employs approximately 51% of the current SPD work force and primarily performs duties of first responder by patrolling the streets of Salinas. Patrol officers are separated into one of four 10-hour patrol shifts to patrol the 12 patrol zones or *beats* (Appendix). Due to recent reductions in forces, SPD routinely dispatches fewer officers than there are patrol beats (Table 5). Additionally, operations may necessitate multiple officers patrolling the same beat, or one officer being assigned to multiple beats (Officer #7, personal communication, January 26, 2011).

[11] This equipment list is specific to the equipment and technology routinely used by patrol officers. SPD does possess additional equipment needed for specific purposes such as analyzing a crime scene or technology used by the computer forensics team. While essential to conducting specific elements of police work, these types of specialty equipment exceed the scope of this research effort and are not included in the analysis of SPD's architecture.

[12] Issuing cell phones to all patrol officers would be cost prohibitive. Currently cell phones are issued to those personnel whose official duties necessitate frequent access to cell phones such as investigators, Watch Commanders, and various supervisors, etc. Patrol officers needing to make a phone call have the choice of either using their personal cell phone or returning to SPD to place the call.

Minimum Staffing Levels for Beat Patrols				
Shift	**Time**	**Weekdays**	**Weekends**	**Special Events**
1st watch	10 Hrs: 07:30 am to 5:30 pm	11 *	11 *	If additional officers are needed for special events, they are hired at their overtime rate and assigned to the event—rather than to patrol a beat.
William watch	10 Hrs: 03:00 pm to 1:00 am	11 *, **	14 *, **	
2nd watch	10 Hrs: 05:00 pm to 3:00 am			
3rd watch	10 Hrs: 10:00 pm to 8:00 am	10*	11 *	
* Since there are more patrol zones than available patrol officers some are assigned to patrol more than one beat				
** The William watch is a subset of the 2nd watch and is composed of approximately six officers who report to work two hours before the 2nd watch to assist with case and call backlogs typically experienced by the 1st watch throughout the day. This is to ensure that the 1st watch can depart work at the end of the assigned shift.				

Table 5. SPD Patrol Staffing Levels

Requests for assistance, or *calls for service*, are received by the dispatch center. Typically, officers are dispatched to an incident location corresponding to the beat they are patrolling. Current policy requires a two-officer response for all emergency calls and one for routine calls. Recent reductions in patrol forces have impacted SPD's ability to meet this two officer response requirement. Depending on the call load of other patrol officers, back up assistance may not be readily available, requiring an officer to respond on his or her own (R. Perrien, personal communication, February 24, 2011). When this occurs, the dispatcher will contact the Patrol Supervisor to determine if an officer should be pulled off a less important call (R. Perrien, 2011). The current fiscal crisis has forced SPD to severely restrict officer responses to non-emergencies. For example, officers are no longer dispatched for:

- minor non-injury traffic collisions
- civil (child custody) matters
- minor nuisance calls, etc.

Additionally, " low priority calls for service are being screened more closely to determine if a police officer is really needed at the scene" (Fetherolf, 2010).

Due to the similarities between patrol officers and military infantry—concerning their first response capability, autonomous nature, and the need for SA—the analysis of SPD's architecture focused on those elements that would best support the efforts of the patrol officer. Additionally, with more than 50% of the sworn officers performing patrol duties, it is the author's belief that aligning a JBAIIC-like architecture with the needs of the patrol officer would result in the most significant improvements for SPD as a whole.

4. A Typical Gang's Communications and Information Architecture

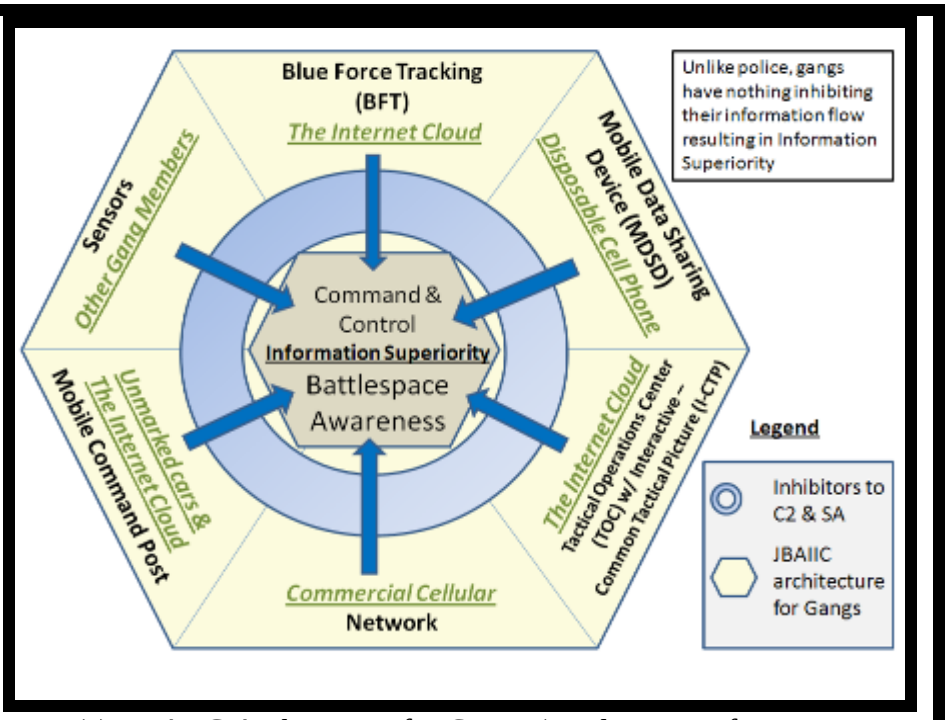
It first must be understood what capabilities criminals currently use to coordinate their activities before attempting to implement a JBAIIC-type architecture so that it can best respond to the threat of violent crime. According to the 2009 National Gang Threat Assessment:

> Gang members often use cell phones and the Internet to communicate and promote their illicit activities. Street gangs typically use the voice and text messaging capabilities of cell phones to conduct drug transactions and prearrange meetings with customers. Members of street gangs use multiple cell phones that they frequently discard while conducting their drug trafficking operations. For example, the leader of an African American street gang operating on the north side of Milwaukee used more than 20 cell phones to coordinate drug-related activities of the gang; most were prepaid phones that the leader routinely discarded and replaced. Internet-based methods such as social networking sites, encrypted e-mail, Internet telephony, and instant messaging are commonly used by gang members to communicate with one another and with drug customers. Gang members use social networking Internet sites such as MySpace, YouTube, and Facebook as well as personal web pages to communicate and boast about their gang membership and related activities. According to open source and local law enforcement reporting, members of "Crips" gangs in Hampton, Virginia, use the Internet to intimidate rival gang members and maintain web sites to recruit new members. On October 23, 2007, a 15-year-old Crips gang member was arrested for shooting a rival gang member in the leg. Additionally, he was charged with the recruitment of persons for a criminal street gang through the use of the gang's social networking site. Gangs in Oceanside, California, are recruiting new members and claiming new turf on the Internet. Gang members flash gang signs and wear gang colors in videos and photos displayed on Internet sites. Sometimes, rivals "spar" on Internet message boards. Oceanside Police Department officers who investigate the city's resident "Crips" and "Bloods," easily find well-produced, self-promoting songs and videos featuring local gang members on Internet web sites. (National Gang Intelligence Center, 2009)

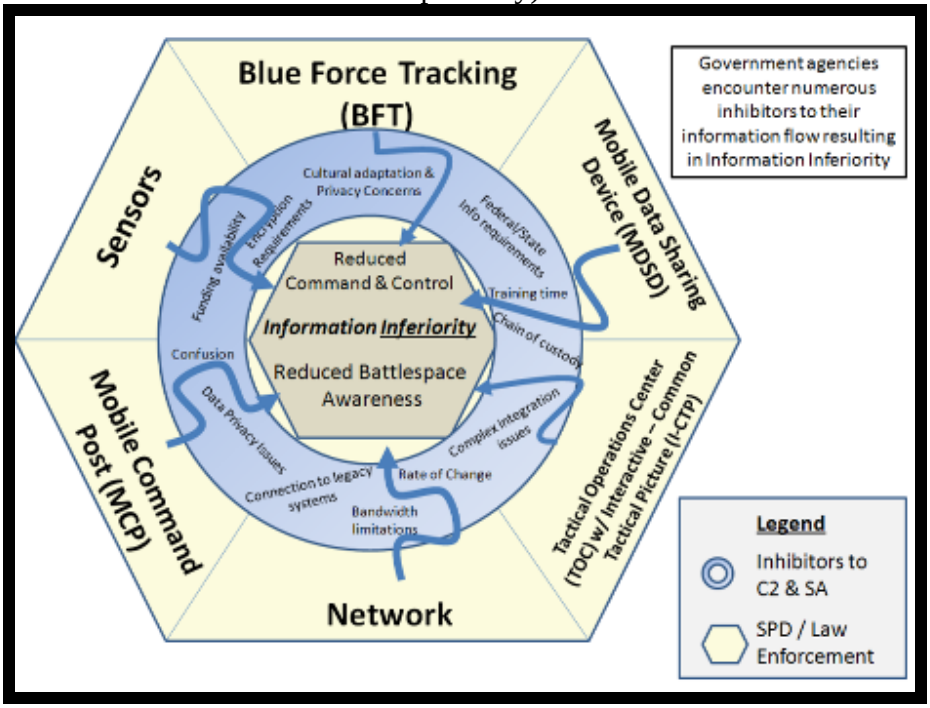
Using these modern social networking methods, gangs are able to recruit, target, and organize illicit activities. The low cost of technology greatly reduces the threshold barrier for those desiring to coordinate illegal activity. As a result, with so few factors inhibiting a gang's ability to access and share information, information technology provides its members a substantial advantage when it comes to using it to support criminal activity.

To combat this threat, SPD officers need similar technological means to access and share information while patrolling in the car or afoot. Additionally, if SPD's architecture is to provide a tactical advantage beyond that possessed by the gangs, all present and future technological initiatives will need to be integrated into a JBAIIC-type

architecture. Comparing the elements of the JBAIIC architecture to architecture used by a typical street gang reveals that gangs can more easily obtain an information advantage over the more encumbered law enforcement agencies (Figure 18).



(a). JBAIIC Architecture for Gangs (resulting in Information Superiority)



(b). JBAIIC Architecture

Figure 18. JBAIIC Architectures for Both Gangs and SPD Resulting in Information Superiority and Information Inferiority Respectively.

As a result, given the challenges facing police concerning accessing and sharing information, and the ease at which gangs can accomplish the same, gangs are able to achieve an information advantage over local law enforcement.

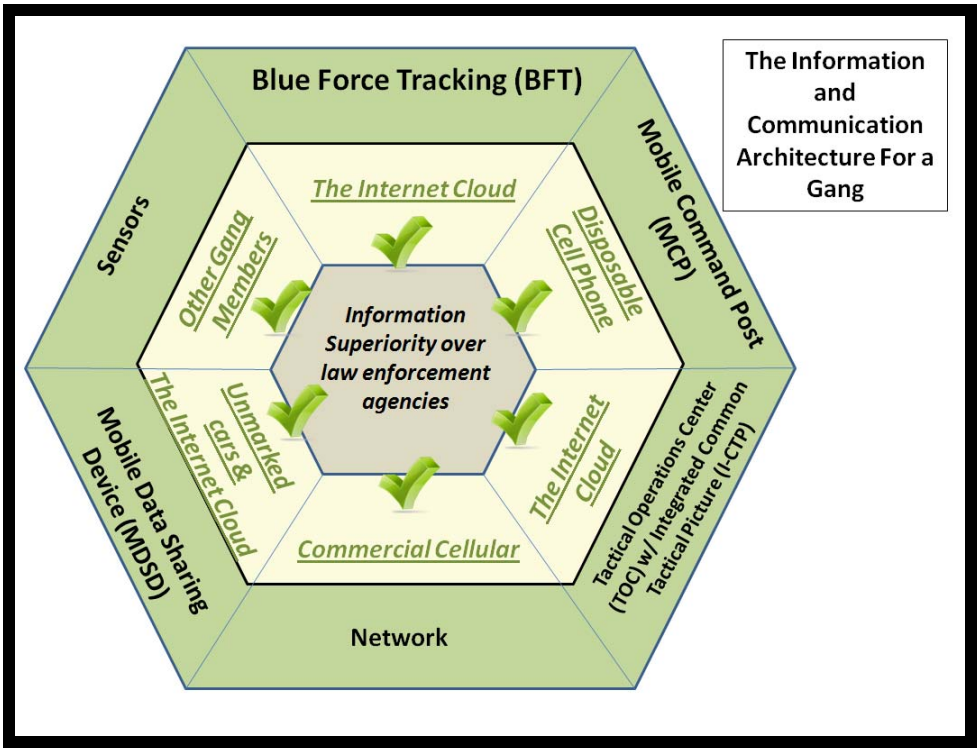


Figure 19. The Ease of Information Access Allows a Gang to Achieve Information Superiority Over Law Enforcement.

III. SPD'S ARCHITECTURE EVALUATION

A. COMPARISONS

Figure 20 provides a general comparison between a Seal Team EIGHT tactical unit and SPD patrol officers. Due to the numerous similarities in mission, tactical units and threat sources, the author believes that the same JBAIIC architecture model used by the Seals is the most appropriate model to assess SPD's architecture.

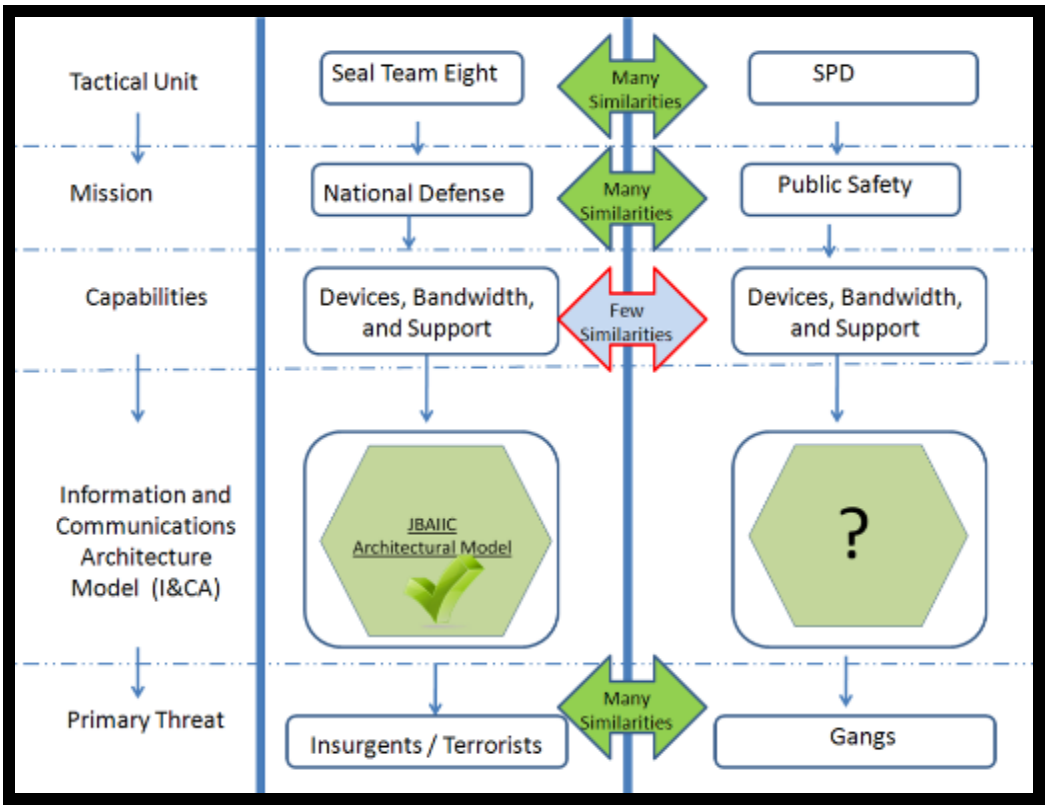


Figure 20. Comparison Between Seal Team EIGHT and SPD.

To conduct the architectural evaluation, we are guided by the model in Figure 21. By matching the existing capabilities of SPD with the six elements of the JBAIIC architecture, researchers and SPD can easily identify factors inhibiting SPD's ability to fight crime. Once completed, a Technology Implementation Plan recommends courses of action to close significant gaps in its present architecture.

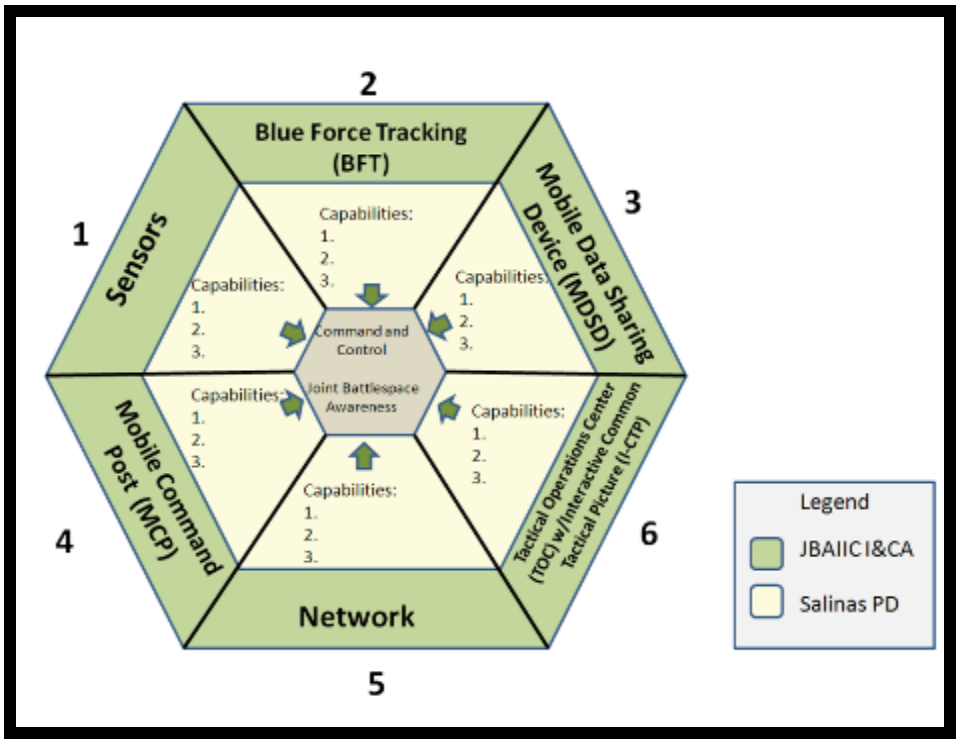


Figure 21. Baseline JBAIIC Architecture Model

Due to the differences between police officers and military infantry, some practical adjustments were made for this analysis. Specifically, the requirement for a JBAIIC architecture to support classified traffic is not appropriate for a police department that does not handle classified information on a routine basis. As a result, the JBAIIC architecture for SPD will need to support only secure (encrypted) and non-secure modes of data transport. Table 4 identifies the JBAIIC characteristics of each architectural element used to evaluate the fit between SPD and JBAIIC's architecture.

The following are the results of the architecture analysis of SPD.

1. Sensors

a. Assessment

(1) Closed Circuit TV (CCTV). Five closed-circuit cameras monitor areas known for frequent crime activity. Four of the CCTVs are portable and one is fixed. The portable cameras allow SPD to relocate them as needed throughout Salinas to monitor emerging threats. The fixed camera is mounted on top of a telephone pole in an area known as China Town. This camera utilizes a FireTide Wi-Fi connection and links directly to SPD via a dedicated T-1 line. The camera video feeds are viewable only at the Watch Commanders desk.

(2) Patrolling officers/vehicles. A minimum of 11 patrol vehicles, with one officer per vehicle, patrol 11 of the 12 predetermined patrol areas. (See Appendix for patrol areas.)

(3) Anonymous crime reporting methods. Two examples include:

- Tip411: Citizens of Salinas act as the sensor by anonymously reporting crime by texting code "SPD831" to "847411."
- WeTip: Citizens of Salinas act as the sensor by anonymously reporting crime via phone (1-800-78-CRIME).

(4) Neighborhood Watch initiatives. Citizens of Salinas act as the sensor by anonymously reporting crime via methods listed above or by dialing 911.

b. Problems

Currently, the sensors monitoring Salinas do not provide adequate persistent sensing. A shrinking police force combined with limited technological sensing capability has significantly degraded SPD's ability to effectively act as the primary sensor for the city. Specific problems include:

(1) Lack of persistent sensing. There is no effective persistent sensor network dedicated to monitoring a large area of the city other than police officers patrolling the streets,

(2) CCTVs. These five cameras work, but they are not actively monitored. Camera video is viewable only from the Watch Commanders Desk at SPD, but daily responsibilities inhibit continuous/effective monitoring.

(3) Anonymous crime reporting methods. Various methods are in place but currently there is no process in place to evaluate its effectiveness.

c. Recommendation

In the absence of a larger patrol force, SPD needs to implement an effective, persistent sensing capability to cover high crime areas. Due to the high levels of violent crime, implementing a gunshot location system (GLS) and expanding the CCTV coverage is strongly recommended. Additionally, streaming the CCTV video throughout the SPD network might create additional opportunities to ensure this data is viewed. However, increasing SPD's sensing capabilities will create even more data to be processed and reviewed. Until more personnel can be added to the force, other internal process changes and/or resource decisions will have to be made in order to create opportunities to review this additional data. Finally, SPD should implement measures to assess the effectiveness of anonymous crime reporting methods. New initiatives impacting SPD's sensing capabilities will be discussed in the Technology Implementation Plan.

2. Blue Force Tracking (BFT)

a. Assessment

SPD does not employ GPS tracking of either its officers or its patrol vehicles and, as such, there are no means to determine the exact location of an officer on patrol. Currently, the only way of determining their location is from the 'Calls for Service Status Board' that is maintained by the dispatch center. Patrol officers can access this

information from the mobile data terminal (MDT) via the MobileCop user interface as shown in Figure 22. From this status board, patrol officers can determine the approximate location of other patrol vehicles.

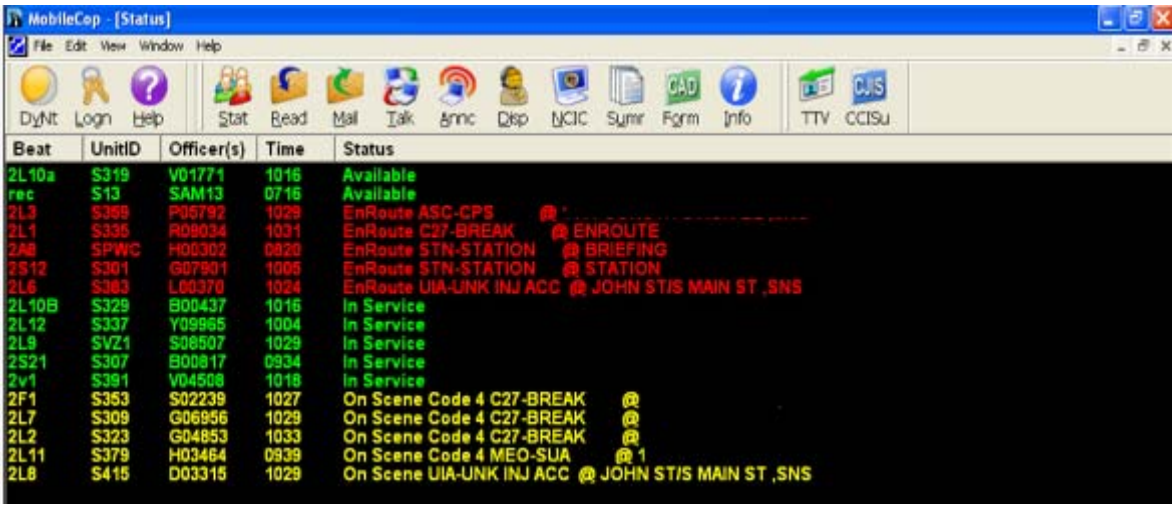


Figure 22. The MDT's MobileCop Status Display Identifying the Location of Patrolling Officers.

b. Problems

The inability to track an officer's exact location is a major safety concern. As SPD's workforce continues to be reduced, individual officers will have to respond more frequently to emergency calls for service that normally requires two or more officers. Depending on the level of activity, it is not uncommon for officers from one beat to be tasked with responding to a call for service in another beat. If an officer's radio malfunctions or if the officer is wounded and unable to communicate their location to dispatch, there is no way of knowing the officer's exact location.

c. Recommendations

For officer safety, SPD should immediately implement BFT for both officers and vehicles.

3. Mobile Data Sharing Devices (MDSD)

a. Assessment

The only MDSDs implemented throughout SPD consists of the vehicle mounted mobile data terminals (MDT), portable magnetic voice recorders, and mobile and portable UHF radios. Other MDSDs in use at SPD include cell phones and iPads; however, neither is issued to patrol officers.

(1) Mobile data terminals (MDT). MDTs used by SPD consist of Panasonic (CF series) laptops with the MobileCop message query and messaging system installed to connect to the dispatch center's Computer Aided Dispatch (CAD) system, see Figure 22. Through this interface, MDTs can access the 'Calls for Service Status Board' as previously mentioned, as well as connect to Federal and State law enforcement databases. MobileCop allows officers to communicate directly with other patrol officers via text message. However, this requires the officer's vehicle to be stopped for safety reasons.

(2) Magnetic tape recorders. These portable devices provide patrol officers the ability to dictate field notes while on patrol and thereby significantly reduce the amount of time officers have to spend behind a desk typing lengthy reports. Once an officer records his/her case notes, the tapes are transferred to the records staff who transcribes the notes into an electronic word processing format.

(3) Portable radios. Patrol officers have access to two radios in the performance of their duties. One mobile radio is mounted in each vehicle and the other is portable handheld radio worn by the officer. These radios are not secure and operate in the public safety frequency spectrum. The vehicle-mounted radios are capable of transmitting data but only at 9600 baud.

b. Problems

The MDSDs used by SPD provide essential capabilities such as instantaneous communications and vehicle-to-vehicle text chat, but lag behind the capabilities of the devices utilized by gangs. For example, once an officer departs a

vehicle, the officer has no access to information resources except by calling the dispatch center or records staff at SPD over the unsecure radio network. Smart phones, netbooks, or PC tablet type devices with appropriate security features could greatly assist officers while away from their vehicles. Cell phones are not currently issued to patrol officers but, due to the need to make frequent phone calls, most officers carry a personal cell phone while on patrol. While this saves SPD the expense of paying for dozens of cell phones and data plans, there is a consequence to this way of doing business. For example, one officer who carries a personal cell phone in the patrol car, stated that when he is required to call someone while on patrol, he will return to the station to make the call via landline to avoid using his/her cell minutes for official business (Officer #4, personal communications, January 26, 2011). The operational impact of officers who might frequently return to the station to make calls is not known. For those officers who do use their personal cell phones, it is unclear if doing so poses a risk to SPD or county IT networks. Finally, the current MDSDs used by SPD do not possess any of the basic characteristics for a JBAIIC MDSD as listed in Table 4.

c. Recommendations[13]

(1) Distribute smart phones or other MDSDs able to access the internet via local cellular networks among the various patrol shifts.

(2) Analyze vulnerabilities of using personal MDSDs. If these risks are acceptable, consider instituting a reimbursement plan for officers who use their personal MDSDs (smart cell phones, etc.) while on duty.

(3) Analyze the operational costs associated with officers returning to SPD to conduct official business that could be accomplished with a MDSD.

(4) Implement MDSDs that meet the minimum requirements listed in Table 4.

[13] SPD has received funding to support the installation of both a new secure radio system and digital voice recorders to assist officers in dictating field notes. As of this writing, neither of these initiatives has been implemented department wide. These initiatives are addressed in the Technology Implementation Plan.

4. Mobile Command Post

a. Assessment

In 2006, SPD integrated an International 4300 as a Mobile Command Vehicle (MCV) into its fleet of response vehicles (Figure 23). MCV's robust design, combined with a deployable camera boom and various multi-media capabilities (TV, radio, DVD, etc.), originally made this vehicle a superb support facility for high-risk events such as hostage and barricade type situations. Currently, MCV is primarily used to support special events such as the annual California Rodeo, parade staging, and DUI processing (Officer #8, personal communications, February 23, 2011). At present, a lack of personnel, the absence of installed computing capabilities, and various equipment casualties have prevented this vehicle from being more fully utilized.

Figure 23. SPD International 4300, Mobile Command Vehicle (MCV). Photo by Detective Michael Groves, Salinas PD

b. Problems

In its current state, numerous equipment casualties prevent MCV from being used more extensively and creates a major tactical disadvantage for SPD. For example, the limited use of MCV reduces opportunities to provide a persistent police presence in high crime areas. Once properly configured, MCV could support the patrol force by providing a significant point of presence in areas of high crime. However, due to

reductions in sworn officers, this would only occur if internal business processes were changed to accommodate personnel working from MCV vice SPD.

The following issues limit SPD's ability to make a greater use of MCV:

- Phone and data usage in MCV require a physical connection. There is no wireless access capability.
- There are no built-in computing capabilities.
- The camera system is incapable of recording video.
- The TV does not receive TV signals, preventing access to news channels for SA.
- The camera boom is not able to remain in the fully extended position.
- A lack of personnel necessitates changes to internal processes to enable those assigned to work in MCV.

c. Recommendation

Repair the identified equipment casualties as soon as possible and incorporate MCV into daily patrol operations in high-risk areas. If SPD is unable implement these repairs, consider staging the MCV in high-risk areas to establish officer presence. Due to recent staff reductions, occupying MCV would require relocating the workspaces of at least two employees. At a minimum, wireless laptops could provide temporary computing capabilities until more permanent workstations could be purchased. Other possibilities include allowing interested groups such as Investigators, Violence Suppression Unit, Gang Task Force, Community Service Officers, or volunteers to incorporate MCV into daily operations.

5. Network

a. Assessment

Wireless Networks. SPD is supported by two wireless networks and is field-testing a third. The two wireless networks in use are the land mobile radio system (LMRS), also known as the County RF system, and Sprint's commercial cellular network that provides service to those officers authorized to carry a cell phones. Additionally,

SPD has begun outfitting patrol vehicles with cellular modems, which will provide Internet access to each patrol car through Verizon's 3G cellular network.

(1) County RF. Patrol vehicles and hand held radios utilize the County Radio Frequency (RF) network to provide communications to the dispatch center. This system is composed of six radio towers located throughout Monterey County and provides non secure 800 MHz UHF voice communications in the public safety frequency band. The data rate for this connection is limited to 9600 baud and connects the vehicle's MDTs to the dispatch center CAD system to exchange text data. This connection allows patrol officers to exchange chat communications between vehicles and conduct database queries. The data rate provided by the LMRS though is too low to support the minimum bandwidth needed to transmit essential information such as mug shots that police could use to identify personnel while on patrol. SPD is pilot testing an initiative to provide an Internet capable data connection to the patrol cars via Verizon's 3G network. As of this writing, no cars have completed this transition but the new wiring has been installed on twenty vehicles.

(2) Commercial Cellular. SPD uses Nextel cell phones that connect to Sprint's local network. Cell phones are not issued to patrol officers but are provided to those personnel whose job requires the use of a cell phone such as the Gang Task Force, Violence Suppression Unit, Investigators, Watch Commanders, and the Chief of Police.

(3) Internet Access in Patrol Vehicles. This initiative and its impact on SPD's capability gaps will be addressed in the Technology Implementation Plan.

b. Internal Network

SPD's internal network is packet switched and provides a 100 Megabit (Mb) connection to each desktop. This network is made up of the printers, desktop computers, and servers that support the department's daily activities. This network is very old and needs major upgrades in order to expand beyond its current capabilities. According to the Salinas' IT manager, "the network is at capacity with no failover

capacity and cannot be expanded beyond its current 2 Gigabit trunked connection without major investments" (S. Golden, personal communication, 11 January 2010). Improving this network would require upgrading the county network as well because the county connection is unable to support anything beyond what SPD currently uses.

c Problems

(1) The lack of secure communications limits SPD's ability to exercise C2 especially during real time pursuits.

(2) The insufficient bandwidth limits a patrol officer's ability to access essential information, such as mug shots, which could slow incident response.

(3) The inability to expand SPD's internal network significantly limits its ability to plan for future technologies that could aide in the fight against crime.

d. Recommendations

SPD should continue its current initiative of installing cellular modems in all patrol cars to provide Internet connectivity to MDTs. Additionally, SPD should meet with city and county IT managers to discuss the future expansion of SPD's network.

6. Tactical Operations Center (TOC) With Interactive—Common Tactical Picture (I-CTP)

a. Assessment 1: Tactical Operations Center

For SPD, the equivalent to a Tactical Operations Center (TOC) is the 911 dispatch center, located at 1322 Natividad Road in Salinas, California (Figure 24). The dispatch center coordinates emergency service responses for the public-safety agencies throughout the county. Every year, the dispatch center receives more than 570,000 calls for service, and initiates emergency responses to more than 150,000 incidents (R. Perrien, personal communication, April 11, 2011).

At the dispatch center, dispatchers are assigned to one of twenty-four workstations organized according to the different jurisdictions throughout Monterey

County. Information from a caller is entered into the Computer Aided Dispatch (CAD) system, which automatically forwards the request to those dispatchers specifically assigned to an emergency service organization such as Fire, Police, EMS (Emergency Medical Services), etc. In addition to these assignments, dispatchers are assigned to "call taking" duties as well. Call takers are the first to answer phones. If a dispatcher is assigned to call-taking duties and is occupied with another call at the time of a new call is received, the call is automatically forwarded to an available dispatcher. Should all dispatchers become occupied, the non-emergency calls will be placed on hold and emergency calls will be answered first. Watch-floor supervisors can assist as needed. At any given time, there are two dispatchers dedicated to supporting SPD (R. Perrien, 2011).

Finally, neither SPD nor the dispatch center employs a full-time crime analyst to review incoming sensor data for the purpose of identifying trends in recent crime activity, or correlating historic events with current cases.

Figure 24. Monterey County's Dispatch Center

b. Assessment 2: Interactive—Common Tactical Picture

At the dispatch center, the equivalent to an Interactive—Command Tactical Picture (I-CTP) is the graphical display in front of each dispatcher. When a

dispatcher receives a call for service, they enter the incident location into the Computer Aided Dispatch (CAD) system, which plots an icon on a Maverick (brand) maps graphical information system (GIS). Unfortunately, the icons displayed on the computer screen frequently do not identify the correct location as entered by dispatchers. This is because the Maverick maps use the centerline of the street to approximate the location of an address instead of a property's parcel number. This process of converting addresses into coordinates on a map is known as geocoding.[14] Additionally, these maps also do not correctly display many of Salinas' specific characteristics such as fire hydrant locations. To remedy this, the dispatch center employs a private contractor part time to update the maps. The dispatch center does not have a 'master' GIS display, but each dispatcher does have the ability to view all activity throughout the various jurisdictions and can change the status of units in other jurisdictions. The GIS display, however, can only be viewed at the dispatch center and cannot be seen at SPD HQ or any other external agencies. The CAD system currently in use in the dispatch center is made by Tiburon version 7.4.1. This system resides on a UNIX mainframe collocated at the facility. In 2015, the current CAD system will reach its scheduled end of life. At that time, the dispatch center will need to shift to the Windows based Tiburon system, called, Command CAD, or transition to an entirely new CAD vendor. Finally, the current CAD system is not integrated with a records management system (RMS). As a result, searching historic crime events for actionable intelligence is a lengthy and cumbersome process.

c. Problems

(1) The inability to view the dispatch center's CAD GIS display at SPD limits SPD's situational awareness.

[14] "Most geocoding in U.S. crime mapping efforts involves interpolation along a line segment stored in a base map. If, for example, a burglary was reported at 125 Madison Street, a geocoding program would determine that the dot should be placed in the middle of the left side of a line segment representing the addresses 101 to 149. The dot is typically offset from the street centerline at a determined distance (25 feet, for example). The logic of interpolation, however, does not always match reality. Not all streets are set up with evenly spaced land parcels of equivalent sizes and not all locales follow the same addressing logic." (J. Markovic, J. Bueermann, K. Smith, 2006)

(2) The inaccuracy of the mapping GIS software with regard to plotting exact locations and correctly displaying Salinas's specific geographical characteristics limits the effectiveness of both the dispatchers and SPD.

(3) The absence of and integrated records management system and full time crime analyst limits situational awareness by preventing SPD from being able to identify emerging threats or changes in recent crime patterns[15].

d. Recommendations

(1) Integrate CAD display into SPD network for viewing on supervisor workstations.

(2) SPD needs to assess the accuracy of the Maverick maps to identify information specific to its needs that is inaccurate or missing. Once done, a prioritized list should be submitted to the county IT department so that its GIS contractor can make the necessary changes.

(3) SPD should petition for a records management system to be included as part of the 2015 CAD replacement project.

[15] SPD is currently in the process of screening applicants to fill a full time crime analyst position.

IV. RESULTS OF THE JBAIIC ARCHITECTURE EVALUATION

SPD's architecture is adequate for providing a public safety presence throughout Salinas, but it is unlikely to achieve the command and control (C2) and situational awareness (SA) needed to resolve its more pressing problem of gang violence. Figure 25 shows the results of SPD's architectural assessment. Red Xs indicate that a given capability does not contribute to the architectures overall ability to achieve C2 and SA and constitutes a capability gap. Green checks indicate that a current capability does contribute to the architectures overall ability to achieve C2 and SA. In short, SPD's capabilities when compared to the baseline JBAIIC architecture do not provide a means of achieving C2 or SA. Those capabilities identified in the diagram are those that had the greatest impact on the assessment.

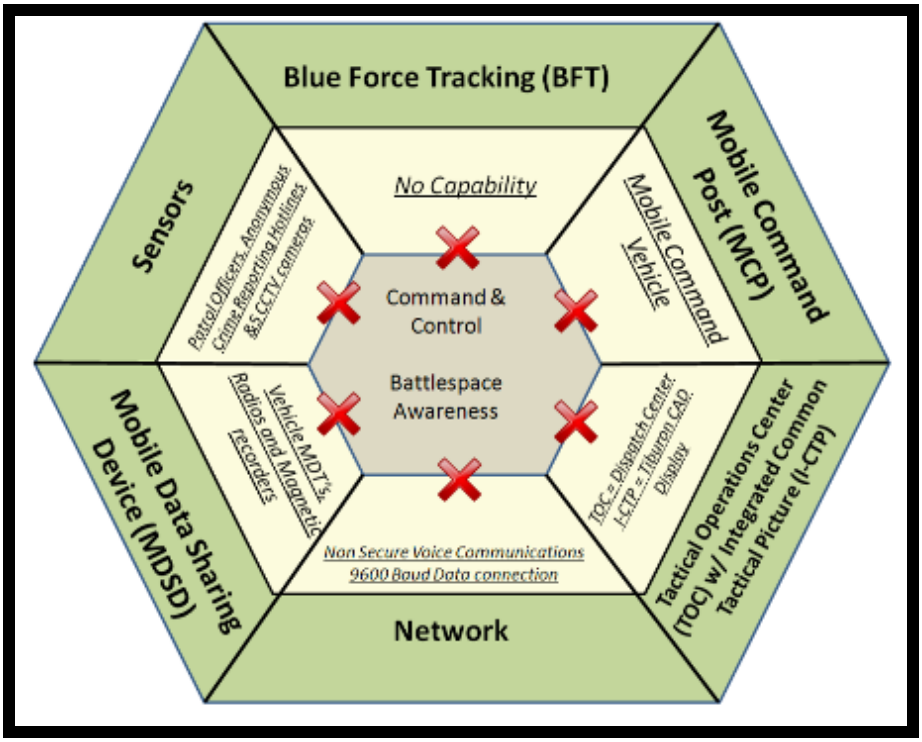


Figure 25. Results of SPD's Architectural Assessment

Throughout the evaluation of SPD's architecture, the two factors that contributed most significantly towards the number of capability gaps were:

A. INCORRECT ARCHITECTURE

SPD's architecture is currently based on its need to provide a public safety presence to the citizens of Salinas. To combat the threat of gang violence though, SPD's capabilities need to be realigned to a JBAIIC architecture that will allow SPD to achieve C2 and SA. Additionally, a tactical architecture such as JBAIIC will help SPD prioritize its resource needs so that new capabilities can be directed immediately towards existing gaps. In the absence of funding support to transition to a JBAIIC architecture, SPD will need to adopt more efficient operational procedures to create the cost savings necessary to afford this transition. The Technology Implementation Plan will identify potential courses of action, which will identify ways to implement a JBAIIC architecture in a resource constrained environment.

B. INADEQUATE TECHNOLOGY

SPD's technology is outdated and less capable than that used by resident gangs. Specifically, it lacks the ability to share relevant and real-time information needed to coordinate actions in response to new crimes or emerging threats. As patrol officers continue to rely on inadequate technology, they will continue to miss opportunities to stop gang violence. Examples include:

- A lack of remote access capabilities necessitates patrol officers frequent return to SPD effectively reducing officer presence throughout Salinas
- Patrol officers do not have access to cell phones requiring them to either return to the station to place a phone call or use their personal cell phones
- While away from their car, a patrol officer's access to information is limited to the availability of the records staff or dispatchers via LMRS
- All communications over the land mobile radio system are non-secure
- The maps used at the dispatch center are not accurate and dispatchers do not have a means of accurately determining officer locations
- The absence of a records management system integrated into CAD limits SPD's ability to more efficiently identify potential crime trends

- Equipment casualties prevent extended use of MCV
- Currently sensing capabilities are capable of persistently monitoring a small fraction of Salinas

Table 6 identifies how SPD's capabilities compare to the minimum capabilities of a JBAIIC architecture.

<table>
<tr><th>JBAIIC Architecture</th><th>Characteristics of the JBAIIC Architecture Elements</th><th>SPD's Significant Results</th></tr>
<tr><td>Sensors</td><td>1. Sensors provide persistent monitoring of battlespace
2. Enough sensors are deployed to cover the battlespace</td><td>1. No - Unknown for anonymous crime tips.
2. No - Too few sensors do not adequately cover crime hotspots</td></tr>
<tr><td>Blue Force Tracking (BFT)</td><td>1. Implemented with GPS
2. Deployed on all assets and personnel</td><td>1. No—No BFT capability
2. N/A</td></tr>
<tr><td>Mobile Data Sharing Devices (MDSD)</td><td>1. Must support both classified and unclassified transfer of data[16]
2. Supports 'push, pull, & share' of data
3. Fully functions in bandwidth limited environment
4. Ruggedized design</td><td><table><tr><th>Question</th><th>Voice recorders</th><th>Radio</th><th>MDTs</th></tr><tr><td>#1</td><td>No</td><td>No</td><td>Yes</td></tr><tr><td>#2</td><td>No</td><td>No</td><td>Yes</td></tr><tr><td>#3</td><td>Yes</td><td>Yes</td><td>No</td></tr><tr><td>#4</td><td>No</td><td>Yes</td><td>Yes</td></tr></table></td></tr>
<tr><td>Mobile Command Vehicle (MCV)</td><td>1. Must support both classified and unclassified transfer of data (see Footnote 16)
2. Direct communications with local units and Tactical Operations Center
3. Redundant Communications
4. Must be fully operational</td><td>1. No - No computing capabilities
2. Yes - Direct comms w/ dispatch center
3. Yes - Five installed radios
4. No – Numerous equipment casualties</td></tr>
<tr><td>Network</td><td>1. Support classified and unclassified data types: audio, video, data. (see Footnote 16)
2. Must be able to communicate with coalition partners</td><td>1. No - Data rate insufficient for Audio and Video data
2. No - LMRS is not P25 compliant</td></tr>
<tr><td>Tactical Operations Center(TOC) with Interactive Common Tactical Picture (I-CTP)</td><td>1. Able to receive classified and unclassified data from sensor network
2. Receives input from all elements of the JBAIIC architecture
3. Displayable for local and external uses
4. Must employ fulltime analysts who fuses sensor data into actionable intelligence</td><td>1. Yes—See Footnote 16
2. No—No input from CCTV video or crime tips reports
3. No—Yes for local, No for external
4. No - SPD is currently screening applicants for crime analyst position.</td></tr>
</table>

Table 6. Significant Results of SPDs Architectural Assessment

[16] For the purposes of this study, the requirement of JBAIIC architecture elements to support classified and unclassified data will be deemed to be met by SPD capabilities able to support secure (encryption) and non-secure modes of data transport.

Figure 26 provides a visual depiction of the capability gaps identified from the analysis as well as a relative comparison of how a specific capability relates to other elements of the JBAIIC architecture. The three circles are used to identify characteristics of a specific capability that matches the minimum JBAIIC characteristics identified in Table 6. The breakdown is as follows:

- Outer red circle: Identifies those capabilities that do not meet any of the minimum JBAIIC architecture characteristics. The section classification *No Capability* is a relative indicator of the capabilities ability to provide C2 and SA.
- Inner yellow circle: Identifies those capabilities that meet at least half of the minimum JBAIIC architecture characteristics. The section classification *Moderate Capability* is a relative indicator of the capabilities ability to provide C2 and SA.
- Center green circle: Identifies those capabilities that meet all of the minimum JBAIIC architecture characteristics. The section classification *Fully Capable* is a relative indicator of the capabilities ability to provide C2 and SA.

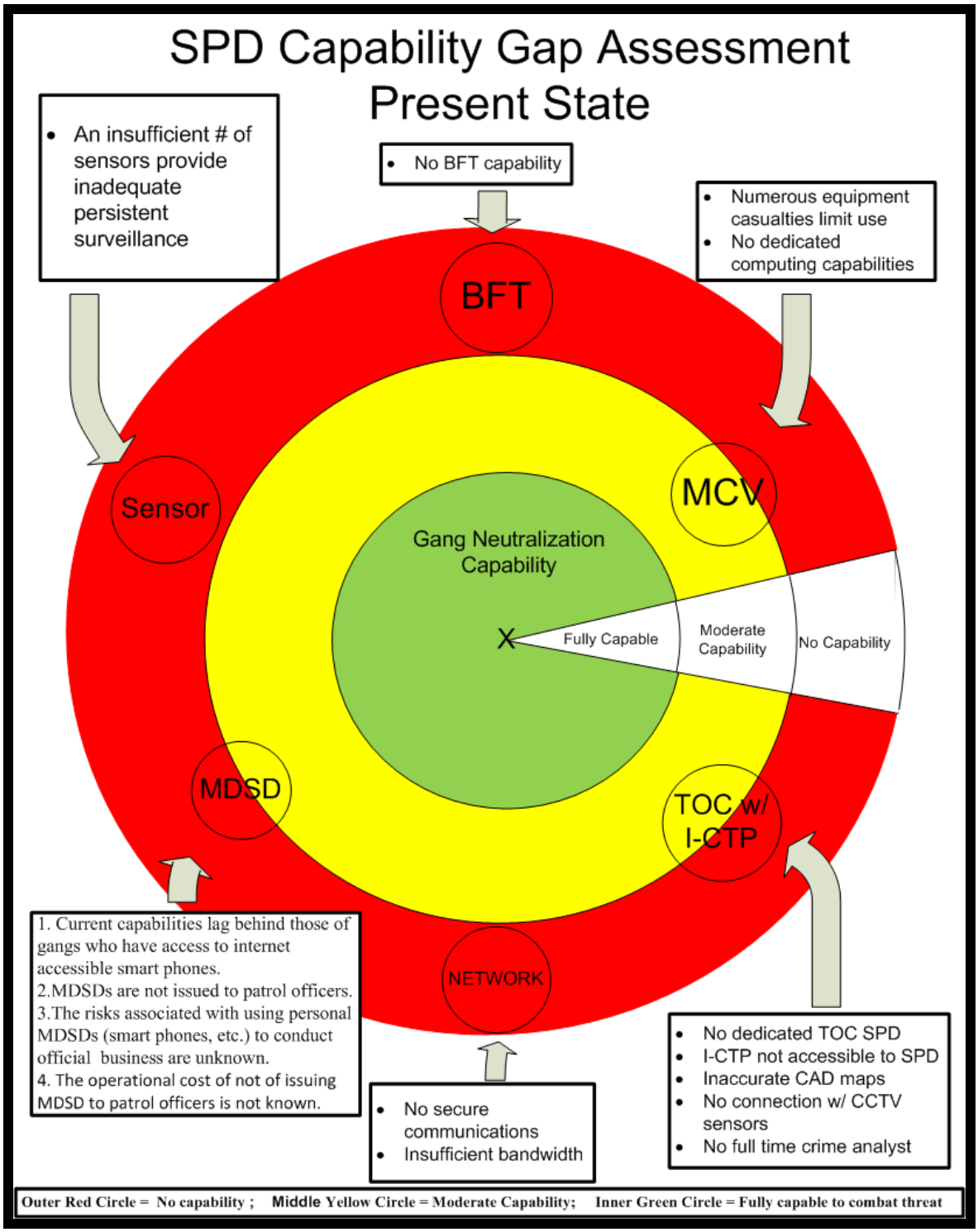


Figure 26. Venn Diagram of SPD's Architectural Capabilities Gaps

To assess the level of integration among the various technologies in use at SPD, rankings of Low, Moderate, and High were used. A ranking of Low was applied to those technologies and capabilities that are isolated and not configured to send or receive information from other devices in the architecture. A ranking of Moderate indicates that approximately half of the devices or capabilities are currently able to access information from other systems. A ranking of High was applied to those devices and technologies that were fully configured and capable of accessing and transporting the desired information. Figure 27 provides a visual depiction of these results.

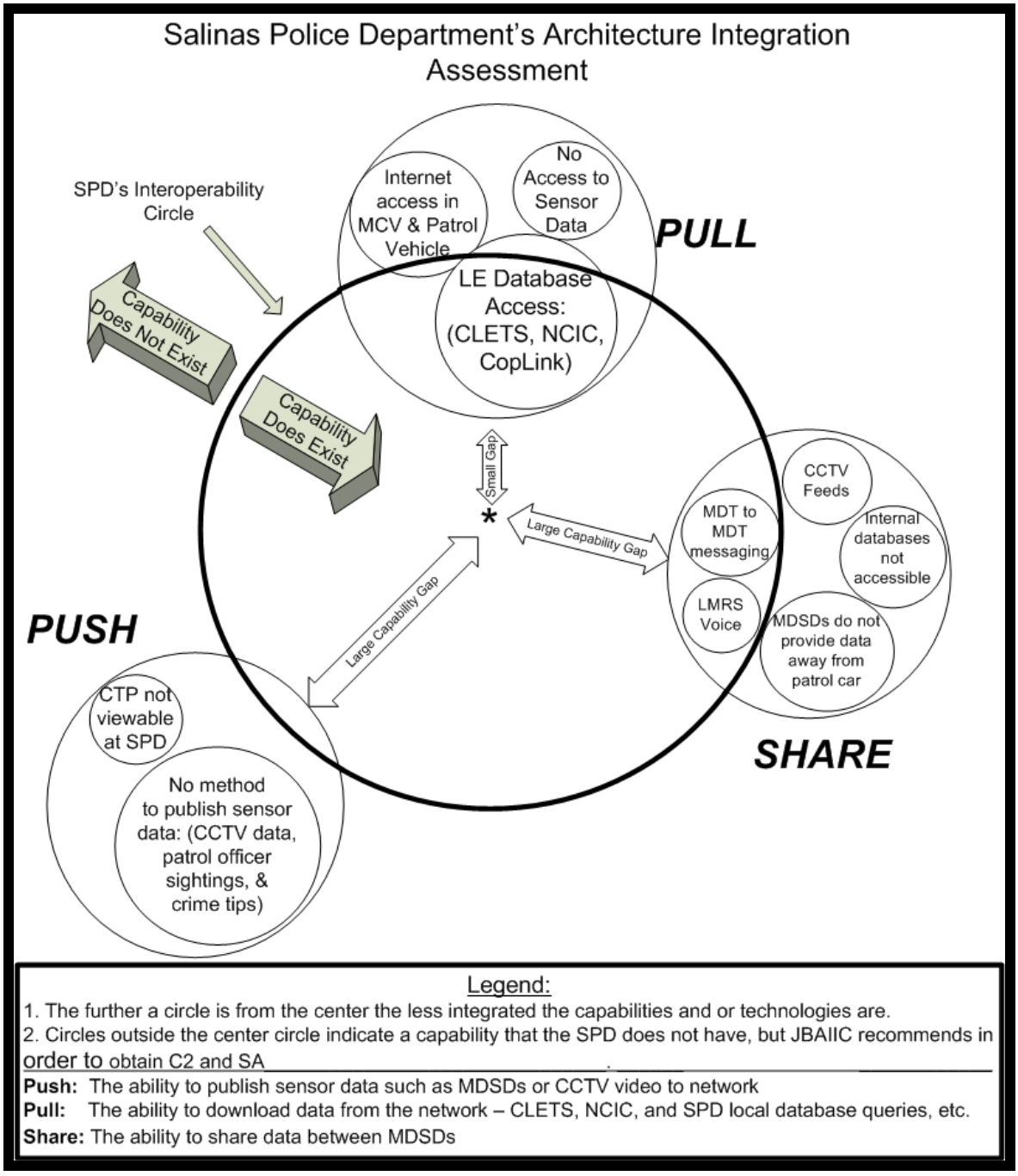


Figure 27. Venn Diagram of SPD's Push, Pull, and Share Capability Assessment

1. Push Capability = *Low*

a. Primary reason for this ranking: Sensor data is broadcast to different locations. Examples include

- CCTV video data is only available at the Watch Commanders desk, which is routinely unmanned
- Actions from patrol officers are only recorded at the dispatch center and on vehicle MDTs but not SPD headquarters
- Anonymous crime tip data is not available at the dispatch center
- CTP display data from the Tiburon GIS at the dispatch center is not available at SPD

b. This gap can be reduced by:

- Ensuring that the above sensor data is available at both the dispatch center and SPD headquarters.

2. Pull Capability = *Moderate*

a. Primary reason for this ranking: Patrol officers have access to essential law enforcement database.

b. This gap can be further reduced by:

- Obtaining Internet access for each vehicle allowing patrol officers to access SPD's local databases (e.g., mug shots and fingerprints)
- Configuring SPD's local databases for remote access from MDSDs

3. Share Capability = *Low*

a. Patrol Officers have no way of disseminating data except through unsecure voice (LMRS), personal cell phones (also unsecure), and text formatted messages on the MDTs (secure).

b. This gap can be further reduced by:

- implementing a means for secure voice communications

- issuing secure MDSDs such as smart phones, iPads, or tablet type devices to all Patrol Officers

To combat this threat, SPD will need technology and an architecture allowing them to access and share information in the same ways that are available to gangs while patrolling in the car or afoot. Additionally, if SPD desires its architecture to provide a tactical advantage beyond that possessed by the gangs, they will need to implement a JBAIIC-like architecture that incorporates all aspects of its present and near future capabilities. Figure 28, shows the recommended JBAIIC architecture for SPD.

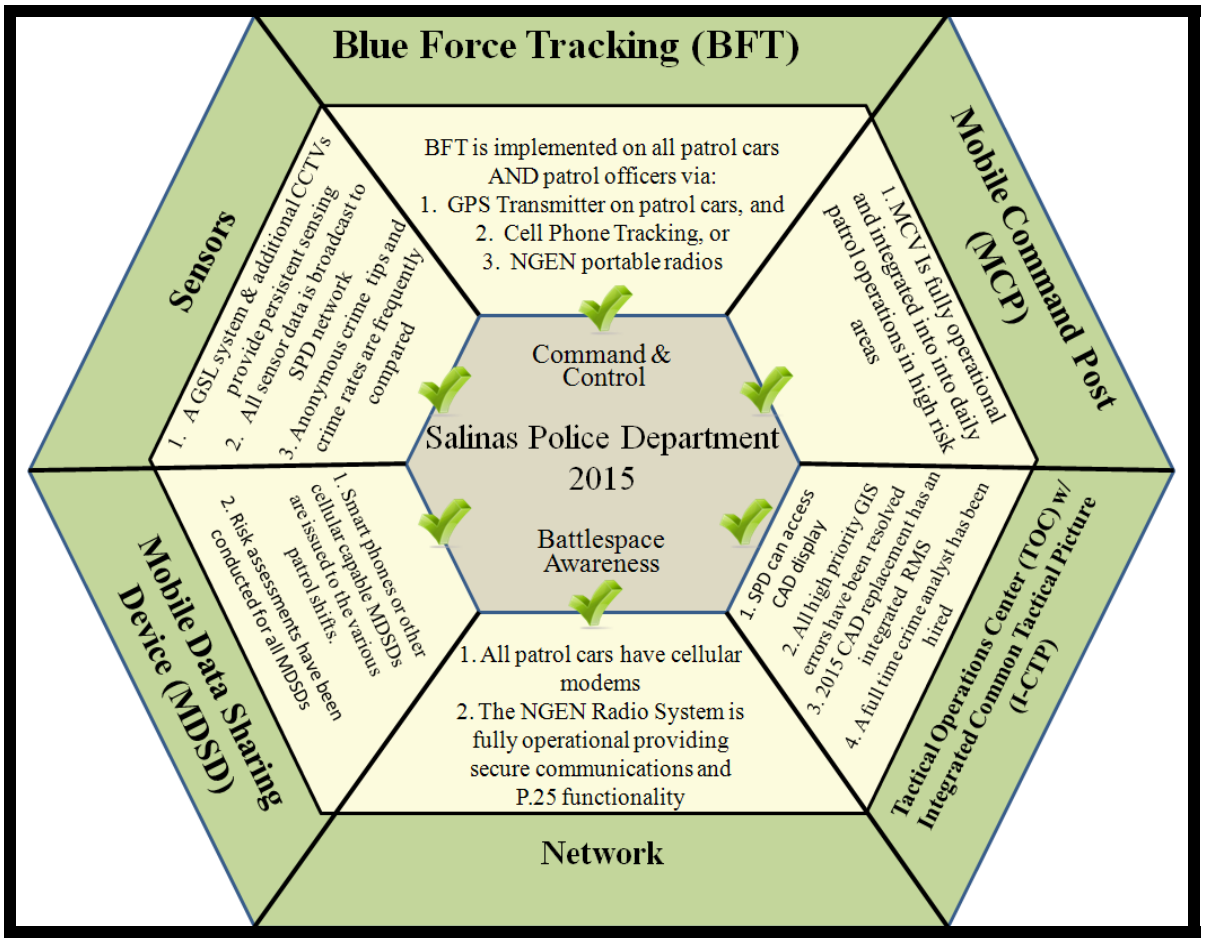


Figure 28. Recommended JBAIIC Architecture for SPD

C. SPD 2015: TECHNOLOGY IMPLEMENTATION PLAN

Based on both the capability gaps identified from the architecture assessment and the significant resource constraints at SPD, a Technology Implementation Plan (TIP) has been created to help SPD transition from its current state to a future state that implements a JBAIIC architecture. This future state is called "SPD 2015" and is represented by the model in Figure 28. This plan starts with a summary of the completed architecture evaluation identifying the significant problems and recommendations as well as the implications of these measures (Tables 7–10). Next, the TIP provides a brief introduction of four technological initiatives occurring at SPD and shows how each impacts SPD's capability gaps. Finally, the TIP concludes with three recommended courses of action for SPD that will put it on the path towards achieving the desired goal of SPD 2015. These courses of action are: #1 Create a Vision to Guide SPD's Technology Initiatives, #2 Implement Business Process Reengineering, and #3 Complete Risk Assessments Prior to Implementing New Technology.

D. SUMMARY OF ARCHITECTURAL EVALUATION

Capability	Problems	Recommendations	Implications
Sensors	1. Sensing capabilities do not provide adequate coverage throughout Salinas. 2. Closed Circuit TV (CCTV) video is not actively monitored. 3. There are no measures in place to evaluate the effectiveness of anonymous crime reporting.	1. Implement persistent sensing methods such as a Gunshot Locations System or increased # of CCTVs. (Problem #1) 2. Stream CCTV video to SPD's private network via multicasting. (Problem #2) 3. Institute measures to validate effectiveness of anonymous tips. (Problem #3)	• Problems #1, #2 & #3: Increased sensing capabilities such as CCTVs will create more data that needs to be reviewed. Changes to SPD's internal organizational responsibilities and processes will be needed to support improvements to SPD's sensing capabilities (Gunshot Locations Systems, CCTV, and anonymous tips).
Blue Force Tracking (BFT)	1. No BFT capability exists at SPD. 2. Emergency response to injured (unable to communicate) officers could be delayed for officers away from their patrol car.	1. Implement BFT throughout SPD on patrol cars and patrol officers via: a. GPS transmitter on the patrol car or other GPS source (Problem #1), and b. Cellular phone tracking (Problems # 1, 2,) until Unity Radios are installed (and have GPS tracking capability) as part of the NGEN project (see section IV.E.3.a.).	• Problems #1 & #2: Implementing BFT at SPD could initially create perceptions of excessive monitoring that might overshadow the need for officer safety.

Table 7. A Summary of the Architectural Evaluation for Sensors and Blue Force Tracking

Capability	Problems	Recommendations	Implications
Mobile Data Sharing Devices (MDSD)	1. Current capabilities lag behind those of gang members who have access to internet accessible smart phones. 2. MDSDs are not issued to patrol officers. 3. The risks associated with using personal MDSDs (smart phones, etc.) to conduct official business are unknown. 4. The operational cost of not of issuing MDSD to patrol officers is unknown. 5. MDSDs used by SPD do not possess the characteristics listed in Table 4.	1. Distribute internet accessible cellular MDSDs to either all patrol officers or to be shared among the various patrol shifts. (Problems #1 & 2) 2. Analyze vulnerabilities of using personal MDSDs. If these risks are acceptable provide MDSDs to patrol officers per recommendation #1 above. (Problem #3) 3. Analyze the operational costs associated with officers returning to SPD to conduct official business that could be accomplished with a MDSD. (Problem #4) 4. Implement only those MDSDs that meet the minimum characteristics in Table 4. (Problem #5)	• Problem #1 & #2: MDSDs issued to all patrol officers could be cost prohibitive and sharing MDSDs among shifts will provide significant savings but will require a device manager to track devices return, maintenance etc. If this is still cost prohibitive, changes in internal business processes could provide the cost savings necessary to support this initiative. • Problem #3: Use of personal MDSDs could impact chain of custody if official records, logs or video are saved on them. MDSDs used by SPD must comply with the Monterey County Device Security Standards Plan. • Problem #4: Instituting a reimbursement plan for officers who use their personal MDSDs (smart cell phones, etc.) while on duty could have a positive impact on SPD resource utilization. • Problem #5: Implementing devices that meet all of these requirements will be expensive and will most likely require some tradeoffs between cost and operational need.

Table 8. A Summary of the Architectural Evaluation for Mobile Data Sharing Devices

Capability	Problems	Recommendations	Implications
Mobile Command Post (MCP)	1. Numerous equipment casualties prevent more frequent use of the MCV creating a significant tactical disadvantage for SPD. 2. The limited use of the MCV reduces opportunities to provide a persistent police presence in high crime areas.	1. Correct all discrepancies and incorporate MCV into daily patrol operations in high-risk areas. (Problem #1) 2. If implementing into daily patrol operations is not possible, consider assigning MCV to other internal divisions that could more frequently use this asset. (Problem #2)	• Problems #1 & #2: Implementing MCV into daily patrol strategies at a minimum would require changing internal business processes such as altering patrol shift routines or relocating personnel workspaces from SPD to MCV.
Network	1. The lack of secure communications limits SPD's ability to exercise C2. 2. Insufficient bandwidth limits patrol officer effectiveness. 3. The inability to expand SPD's internal network significantly limits its ability to plan for future technologies that could aide in the fight against crime.	1. Implement a secure means of communicating. *Note: The NGEN Radio System will provide secure communications.* (Problem #1) 2. Expedite installation of cellular modems to all patrol cars for Internet access. (Problem # 2) 3. Meet with city and county IT officials to discuss expansion of SPD's network. (Problem #3)	• Problem #1: Secure communications will create new ways of coordinating strategic operations. • Problem #2: Increasing the access to information in the patrol car could reduce sensing capabilities because officers will be able to get more administrative work done from the patrol car. • Problem #3: Increasing SPD's network capacity will reduce the likelihood of catastrophic loss of essential data in the event the network is damaged.

Table 9. A Summary of the Architectural Evaluation for Mobile Command Vehicle and Network

Capability	Problems	Recommendations	Implications
Tactical Operations Center (TOC) with Interactive - Common Tactical Picture (I-CTP)	1. The inability to view the dispatch center's CAD GIS display at SPD limits situational awareness. 2. Inaccurate GIS maps limit effectiveness of dispatchers and SPD. 3. The dispatch center's CAD does not have an integrated records management system (RMS). 4. Neither the dispatch center nor SPD have a full time crime analyst.	1. Integrate the CAD display into SPD's network for viewing on supervisor workstations. (Problem #1) 2. Provide county IT division a prioritized list of GIS mapping corrections. (Problem #2) 3. Petition for a records management system (RMS) to be included as part of the 2015 CAD replacement project and hire full time crime analyst. (Problems #3 & 4)	• Problem #1: Having access to the dispatch centers CAD display would improve a patrol officer's ability to recognize new crime hotspots. • Problem #2: Accurate maps will improve incident response. • Problem #3 & #4: A crime analyst supported by an integrated RMS, could more easily identify crime trends, activity hotspots and emerging threats throughout the city. SPD is currently in the process of screening applicants for a full time crime analyst.

Table 10. A Summary of the Architectural Evaluation for Tactical Operations Center with Interactive Common Tactical Picture

E. CURRENT TECHNOLOGY INITIATIVES

1. Technology Initiative #1: Transitioning from Magnetic Tape Recorders to Digital Recorders Via the iPod Touch

Figure 29. Screen Capture of Pocket Dictate Digital Voice Recording Application Using the iPod Touch v.4 (From NCH, 2011)

a. General Information

SPD has received a grant to replace its aging magnetic tape recorders with digital recorders. Currently, patrol officers dictate case notes into a magnetic recorder while on patrol and upon returning to the station, hand the tape(s) over to the records staff where they are transcribed into case logs. The iPod Touch v.4 has been chosen as the replacement for the tape recorders. To provide voice-recording capabilities, SPD will use the PocketDictate application, version 5.19, by NCH Software. The iPod Touch is a portable media player and personal digital assistant that uses Wi-Fi to connect to the Internet. These devices will provide patrol officers the ability to email saved recordings to the records staff without having to return to the station, as long as they have access to a

Wi-Fi network. There are thousands of applications, or "apps," currently available for the iPod Touch. As a result, this device could be used in numerous additional ways beyond that of a voice recorder.

b. Specific Details

Table 11 identifies additional details concerning this initiative.

JBAIIC Architecture Category	**Mobile Data Sharing Device (MDSD)**
Problems Addressed (As taken from the MDSD section of the Summary of Architectural Evaluation Table 8).	• The use of iPod Touch's fully resolves problem #2 and satisfies recommendation #1. • The use of iPod Touchs partially resolves problem #1. The need to have access to a Wi-Fi hotspot prevents resolution of this problem.
Capabilities Gained	• Mobile Internet Access (at Wi-Fi hotspots) • Full push, pull, and share of data between patrol officers (Video Conferencing (among similar devices), email, etc.) when connected via Wi-Fi. The device functions in a bandwidth limited environment and can be ruggedized with accessories.
Limitations	Patrol officers will need to locate available Wi-Fi hotspots to transmit data to SPD or other officers.
Planned Start Date	May 2011
Planned Completion Date	None Specified

Table 11. Specific Details of the iPod Touch

c. Comments

(1) The use of the iPod Touch represents a significant technological enhancement to SPD's MDSD capabilities. While these devices offer tremendous potential for SPD, its advanced capabilities and portability require special considerations regarding both device management and potential introduction of vulnerabilities into SPD's network. For example, these devices can access the internet through publicly available Wi-Fi hotspots and, therefore, will operate outside of the protective boundary of

the city and county's secure IT network. This means that SPD will have to assume the additional responsibility of ensuring that appropriate security safeguards, such as data encryption, are properly implemented. Until the risks associated with its use are fully assessed by SPD, it could be a source of disruption to SPD's operations.

(2) These devices only transmit data via Wi-Fi. As a result, officers using them will need to frequent the numerous Wi-Fi hotspots throughout Salinas. These hotspots are open to the public as well as those at local business and could be used after obtaining the network password (with permission of the operator). Consideration will need to be given as to whether this poses a threat to patrol officers who might frequently return to the same location throughout a shift to transmit data files.

d. Recommendations

(1) The use of iPods as a replacement for magnetic tape recorders is an excellent idea but one that should not be rushed. SPD should not implement the use of iPods until COAs #1 (Vision), #2 (Business Process Reengineering), and #3 (Conduct Risk Assessments) have been completed. Completing these courses of action will ensure this technology is properly implemented so as to make best use of its multipurpose architecture.

(2) Do not use publicly available Wi-Fi hotspots to transmit voice recordings unless appropriate security (encryption) measures are in place. Until such time, have officers upload data when returning to SPD as part of their normal patrol duties.

(3) As more uses for this device are discovered, conduct risk assessments for each intended use.

e. Impact on Capability Gap

Once internal risk assessments are completed (see Course of Action #3), the iPod Touch could significantly reduce the capability gap in the Mobile Data Sharing Device category of the JBAIIC architecture. This device is capable of meeting all elements of the characteristics specified in Table 4. Figure 30 shows the impact the iPod

Touch could have on the MDSD capability gap. If properly implemented this device could provide enhanced operational capabilities to SPD.

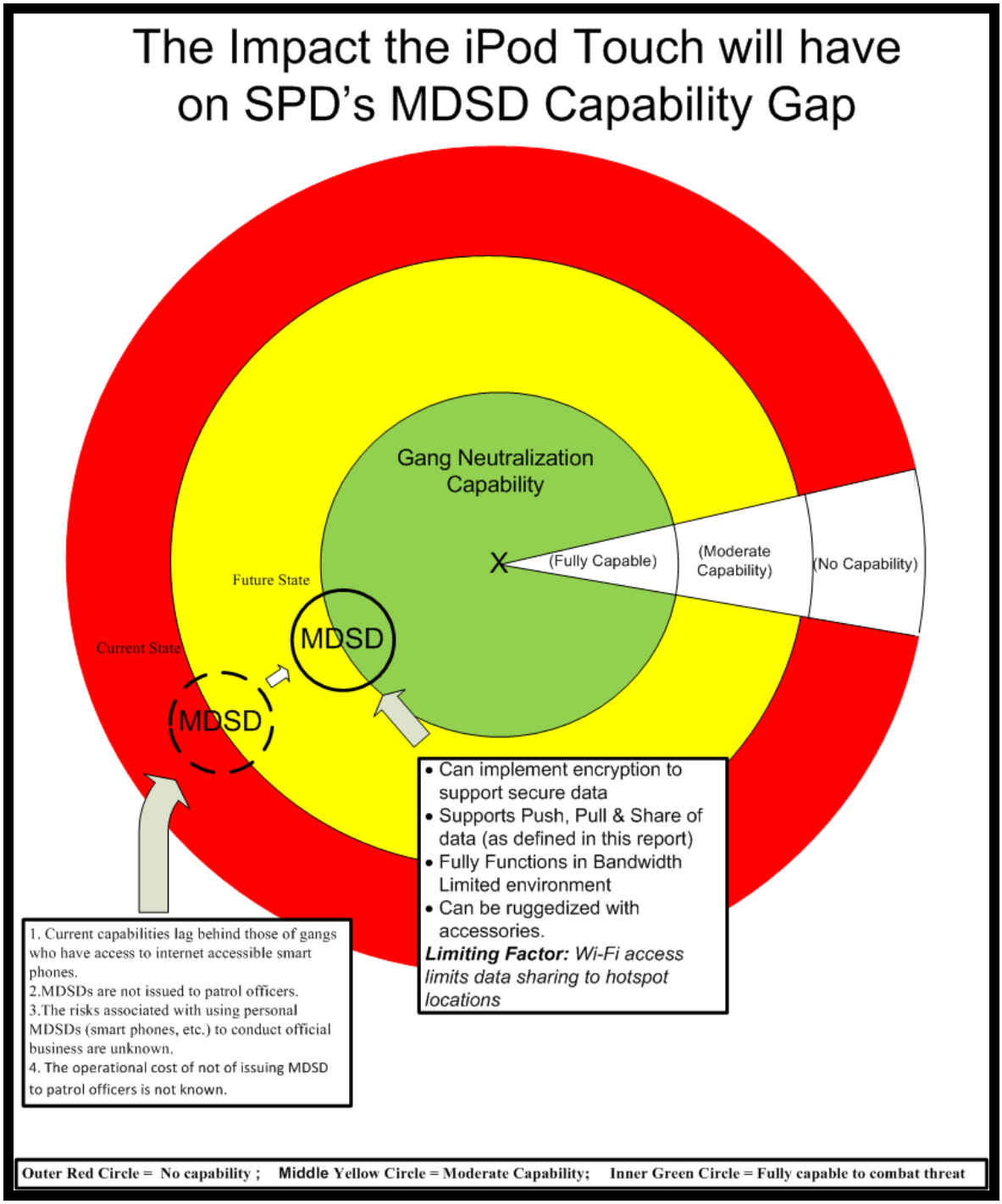


Figure 30. Use of an iPod and Its Impact on SPD's MDSD Capability Gap

2. Technology Initiative #2: Providing Internet Access to Patrol Cars Via Verizon's Commercial Cellular Network

a. General Information

SPD is currently in the process of configuring all patrol vehicles with wireless Internet access as a result of receiving a grant from the Edward Byrne Memorial Justice Assistance program. This project will transition the data connection from the current analog land mobile radio system to a digital cellular connection that utilizes Verizon's local cellular network. When completed, this project will provide significantly increased bandwidth to the mobile data terminals (MDTs) located in each patrol car. Currently several vehicles are testing this technology and wiring has been installed on 20 vehicles. This will be a private network that is not accessible to the general public.

b. Specific Details

Table 12 identifies additional details concerning this initiative.

JBAIIC Architecture Category	**Network & Mobile Data Sharing Device**
Problems Addressed (As taken from the Network and MDSD section of the Summary of Architectural Evaluation Tables 8 and 9).	The transition to cellular network will resolve problem #1 in the Network Category and #4 in the MDSD category.
Capabilities Gained	• Internet Access • Increased Bandwidth
Planned Start Date	In Progress
Planned Completion Date	Summer 2012

Table 12. Specific Details of the Implementation of Cellular Modems

c. Comments

(1) The most significant capability of this new configuration will be the ability of patrol officers to connect to the SPD local network while on patrol. Patrol officers will be able to access local databases, personal work files, and all applications

available to officers at SPD. Connecting to SPD's network will require using Citrix Remote Access software, which is installed and maintained by the city of Salinas Information Technology Department (ITD).

(2) The MDTs that have are participating in the testing phase have been configured in such a way that prevents them from simultaneously connecting to the Internet and the various law enforcement databases accessed through the country network. This prohibition is per policy of the Department of Justice to prevent viruses and other malware located on the Internet from infecting the servers that support the various law enforcement databases. This policy is enforced by the county ITD and requires configuring the Radio Internet Protocol (IP) Server to lock down the IP stack preventing dual use or split tunneling of the MDT's IP address (J. Crane, personal communication 26 January 2011). Tests of this configuration revealed very slow connections while utilizing the Citrix connection. As a result, the County ITD is requesting permission from the DOJ to allow split tunneling. If this is authorized, the County ITD will implement appropriate security protocols to ensure no vulnerabilities from the Internet are introduced into the network.

d. Recommendations

SPD will need to educate the patrol force regarding possible ways Internet access could introduce viruses or other malicious software into both the city and county networks.

e. Impact on Capability Gap

The transition to a commercial cellular network provides a significant increase in both information access and information sharing capabilities to the patrol officer (Figure 31). Due to the significant increase in bandwidth provided by the cellular network, officers will be able to incorporate new functionality to their field operations. Examples include:

(1) Direct access to the local mug shot database will provide a more expeditious means of having victims positively identify their assailant. Also, mug shots can be instantly shared among patrol officers participating in the search for a wanted person resulting in increased situational awareness (SA).

(2) The use of wireless access will provide the Chief of Police the means to implement Blue Force Tracking (BFT) like capabilities. While not as accurate as GPS, position tracking via cellular technology will allow the SPD to experiment with the tactical and SA capabilities that BFT could provide while increasing officer safety at the same time.

(3) Patrol officers would be able to monitor the video feeds from SPD's CCTV network and immediately respond to suspicious activity.[17]

(4) Internet access in patrol vehicles will enable the use of video conferencing technology. With this technology, patrol officers can virtually attend operations meetings or communicate with other patrol vehicles via video chat.

[17] Viewing CCTV video from the SPD's wireless cameras would require enabling the multicasting functionality on the cameras, routers, and server.

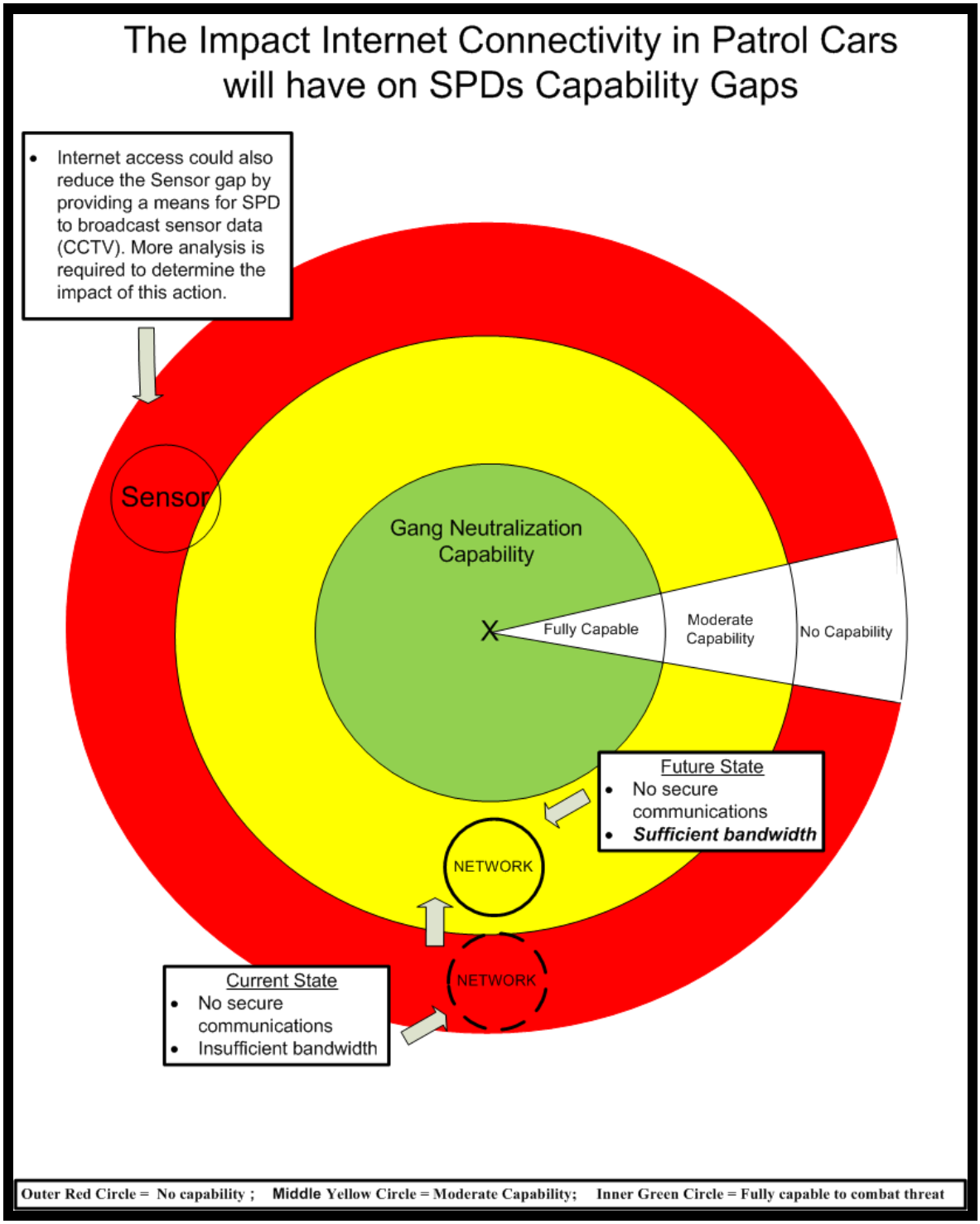


Figure 31. Impact of Internet Access on SPD's Capability Gaps

3. Technology Initiative #3: Monterey County Next Generation Public Safety Communications System

a. General Information

The County of Monterey awarded a $15 million dollar contract to the Harris Corporation to upgrade its legacy land mobile radio system (LMRS). The project, called NGEN, for Next Generation Radio, will add improved interoperability, enhanced coverage, and new functionality to the communications capabilities of the public safety organizations throughout Monterey County (Dillon, 2011). This project will introduce the XG-100 Unity portable and mobile radios; full-spectrum multiband radios that provide first responders with secure communications and Bluetooth capability. In addition, these radios meet the FCC Narrowband[18] requirements and comply with phase one and two of the P25[19] industry standard. Table 13 identifies additional details concerning this initiative.

b. Specific Details

JBAIIC Architecture Category	**Mobile Data Sharing Device & Network & BFT**
Problems Addressed (As taken from the MDSD and Network section of the Summary of Architectural Evaluation Table 7).	• Network (Problem #2)—NGEN provides secure communications • BFT (Problems #1 and #2)—Officers will be able to locate other officers
Capabilities Gained	• Secure Communications • BFT via GPS[20], and Bluetooth for hands free use • Regional interoperability due to P25 compliance
Planned Start Date	June 2011
Planned Completion Date	Dec 2011

Table 13. Specific Details of the NGEN Implementation Project

[18] FCC has made *narrowbanding* a requirement to "promote more efficient use of the VHF and UHF land mobile bands" (Bercovici, 2006).

[19] Project 25 (P25) is a collection of "standards that allow radios and other components to interoperate regardless of manufacturer—enabling emergency responders to exchange critical communications" ("P25 Compliance", 2006).

[20] GPS position data is displayed on a small screen on the XG-100 P and M models. Currently these radios are not capable of sending GPS data to a external source such as a Tactical Operations Center but Harris is currently in the planning process to provide this functionality in the future (B. Wood, personal communication, March 14, 2011).

c. Comments

The NGEN project will provide substantial improvements over the existing LMRS. Of the many improvements, SPD will now be able to communicate securely without the fear that their communications are being monitored. This new capability will provide a strategic advantage for SPD's patrol officers responding to gang violence.

d. Recommendations: None

e. Impact on Capability Gap

Once installed, and when combined with the benefits of Internet access, NGEN will completely reduce the capability gaps in the Network category (Figure 32). Additionally, the BFT gap will also be eliminated once enhanced GPS functionality is implemented by Harris. NGEN will also reduce the MDSD and MCV capability gaps to a lesser extent

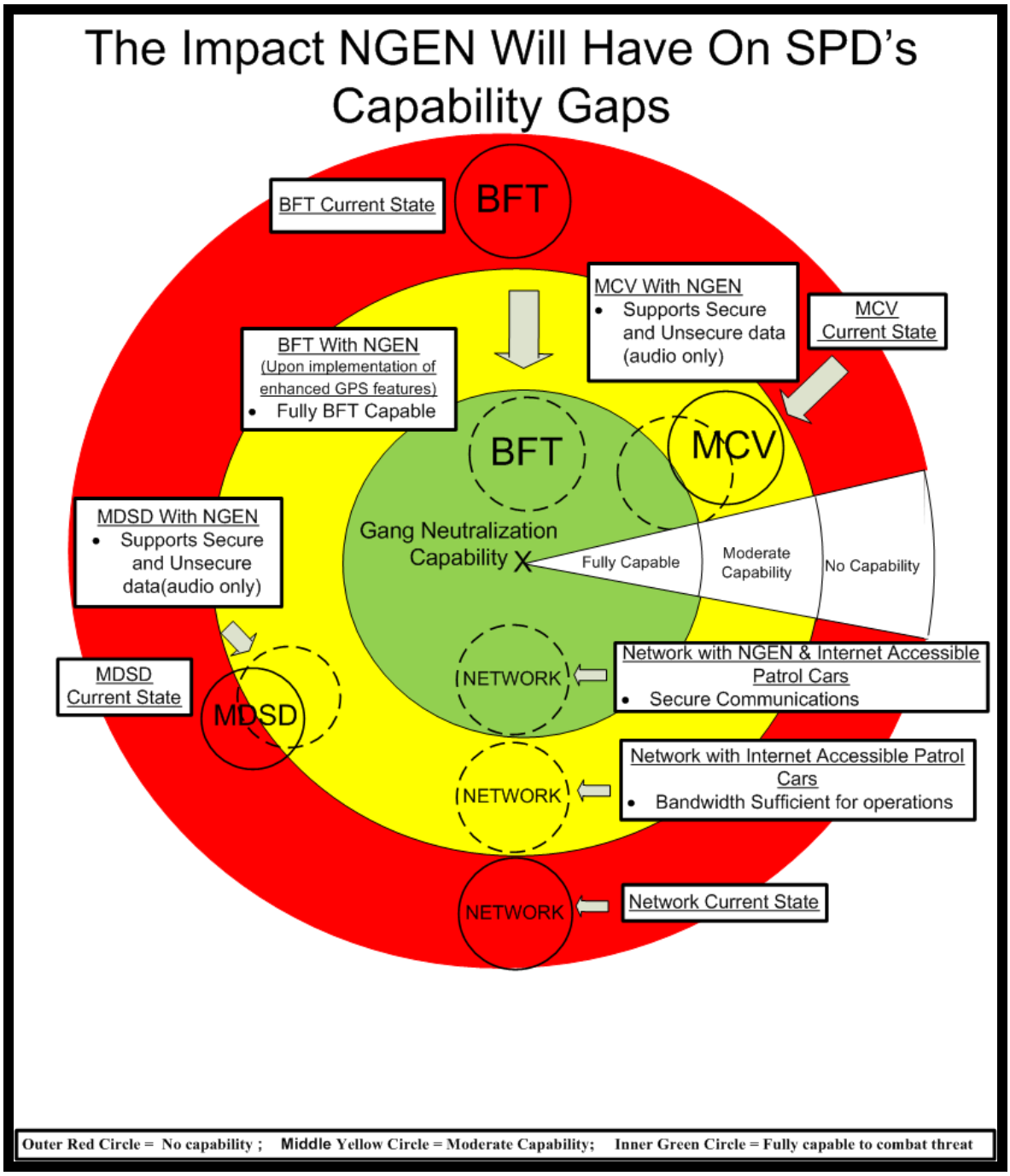


Figure 32. Impact of Unity Radios on SPD's Capability Gaps

4. Technology Initiative #4: ShotSpotter's Gunshot Location System

a. General Information

In partnership with the Naval Postgraduate School, the Salinas Police Department is in the process of implementing ShotSpotter's gunshot location system (GLS) into its arsenal of crime fighting capabilities. This system uses acoustic sensors to detect and locate gunshot and explosive events in real time (ShotSpotter, 2011). Approximately 50 sensors will be installed in a three square mile in East Salinas, an area known for high crime (Figure 33). Upon detecting an event, sensors will transmit the data to ShotSpotter's Mountain View, CA headquarters, where trained staff will analyze the events acoustic characteristics. Those events classified as potential gunfire or explosions will be forwarded to the dispatch center for action. The system is anticipated to be operational in summer 2011 and will provide SPD the following actionable data:

- Nearest street address
- Time of event
- Incident type (Gunfire, explosion, firework, or non-threatening sound)
- Audio clip
- Path of travel, in the case of mobile shooter(s) (ShotSpotter, 2011)

Table 14 identifies additional details concerning this initiative.

Figure 33. Anticipated Coverage Area of ShotSpotter's Gunshot Location System (From Google Maps, 2011)

b. Specific Details

JBAIIC Architecture Category	Sensor
Problems Addressed	1. Lack of persistent sensing (problem # 1) 2. Anonymous crime reporting effectiveness (problem #3)
Capabilities Gained	1. Persistent sensing in an area known for violent crime 2. Verification of the effectiveness of SPD's anonymous crime methods.
Planned Start Date	Summer 2011
Planned Completion Date	July 10, 2011

Table 14. Specific Details about ShotSpotter's Gunshot Location System

c. Comments

A gunshot location system brings many opportunities to SPD and is an exceptional and much needed sensing resource. With this system, SPD will be able to accurately determine the boundaries of high-risk areas as well as provide a much reduced response time to both reported and unreported gunshot events. Additional issues specific to the implementation of GLS technology include:

- The accuracy of the system will enable SPD to experiment with various methods of targeted enforcement.
- Certain annual events such as the Fourth of July and New Year's Eve will provide SPD opportunities to demonstrate and educate the general public as to the capabilities of GLS technology.
- The location of events detected outside of the boundaries of a coverage area decreases the further away the event is from the coverage area. These events might require a different response strategy.
- The location of events might necessitate changes to beat boundaries or minimum officer response requirements.

The most significant challenge SPD will have with the ShotSpotter GLS is paying for the annual 120K (estimated) subscription fee. The Naval Postgraduate School received a grant from the Department of Homeland Security to pay for the installation and a one-year service plan as part of a research effort. At the end of one year, if SPD desires to continue using the system funding will need to be provided or the GLS services will be terminated.

d. Recommendations

Due to the limited one-year service agreement, SPD should assign a Project Manager capable of enforcing installation preparations as well as monitoring system performance throughout the first year.

e. Impact on Gap

A gunshot location system will significantly reduce SPD's sensor capability gap (Figure 34). By having numerous sensors distributed throughout high crime areas, SPD will be able to continuously monitor and respond to events. With this

system, SPD will no longer be reliant on the citizens in the gang-controlled areas of East Salinas to report shootings. As a result, despite recent staff reductions, SPD's quick response to gunshot events will create the perception of a larger and more effective police force.

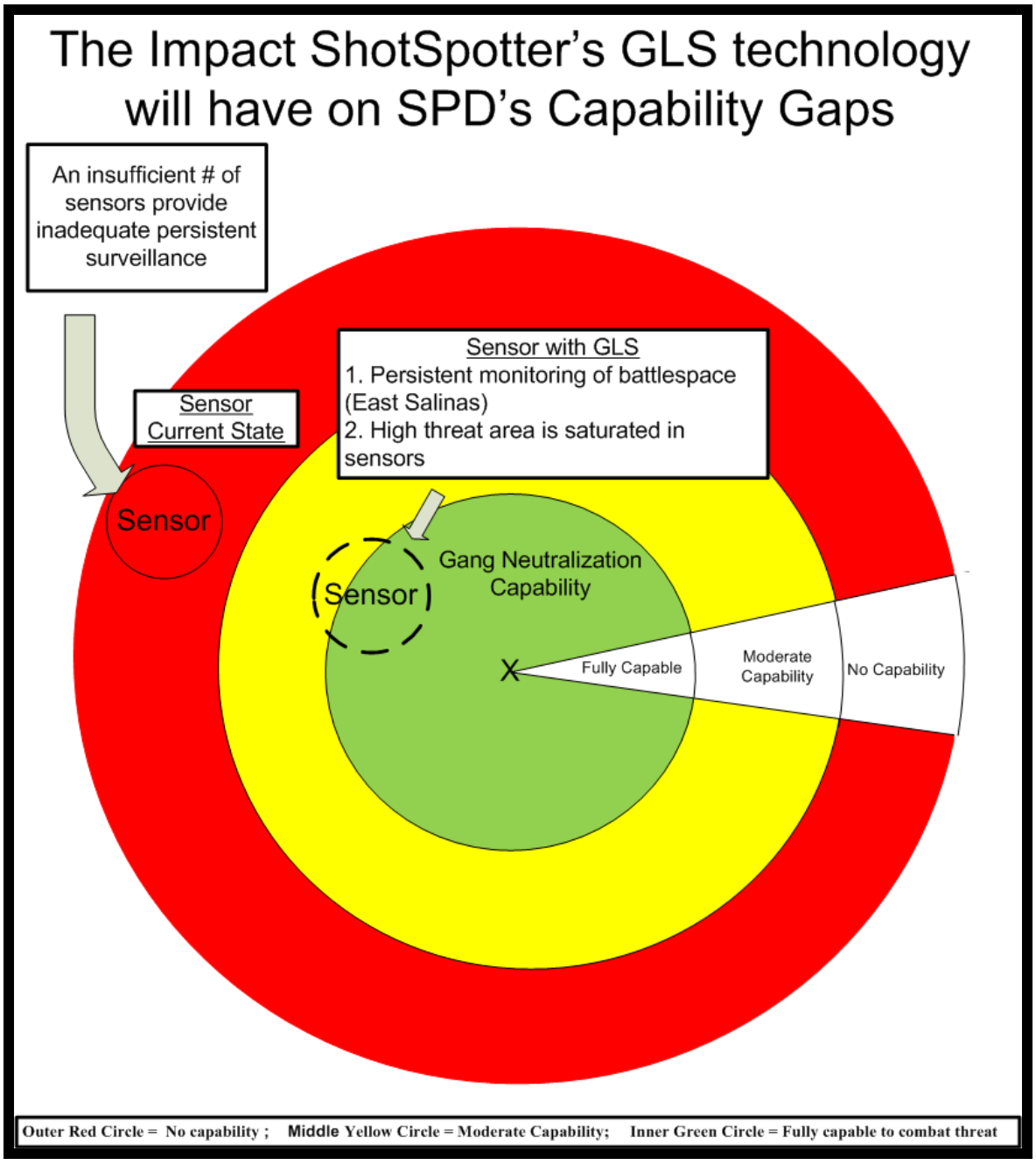


Figure 34. The Impact of ShotSpotter's GLS on SPD's Capability Gaps

F. COURSES OF ACTION

To assist SPD in transitioning from its present architecture to that of a JBAIIC-like architecture called SPD 2015, three courses of action are suggested:

- #1 Create a Vision to Guide SPD's Technology Initiatives
- #2 Implement Business Process Reengineering
- #3 Complete Risk Assessments Prior to Implementing New Technology

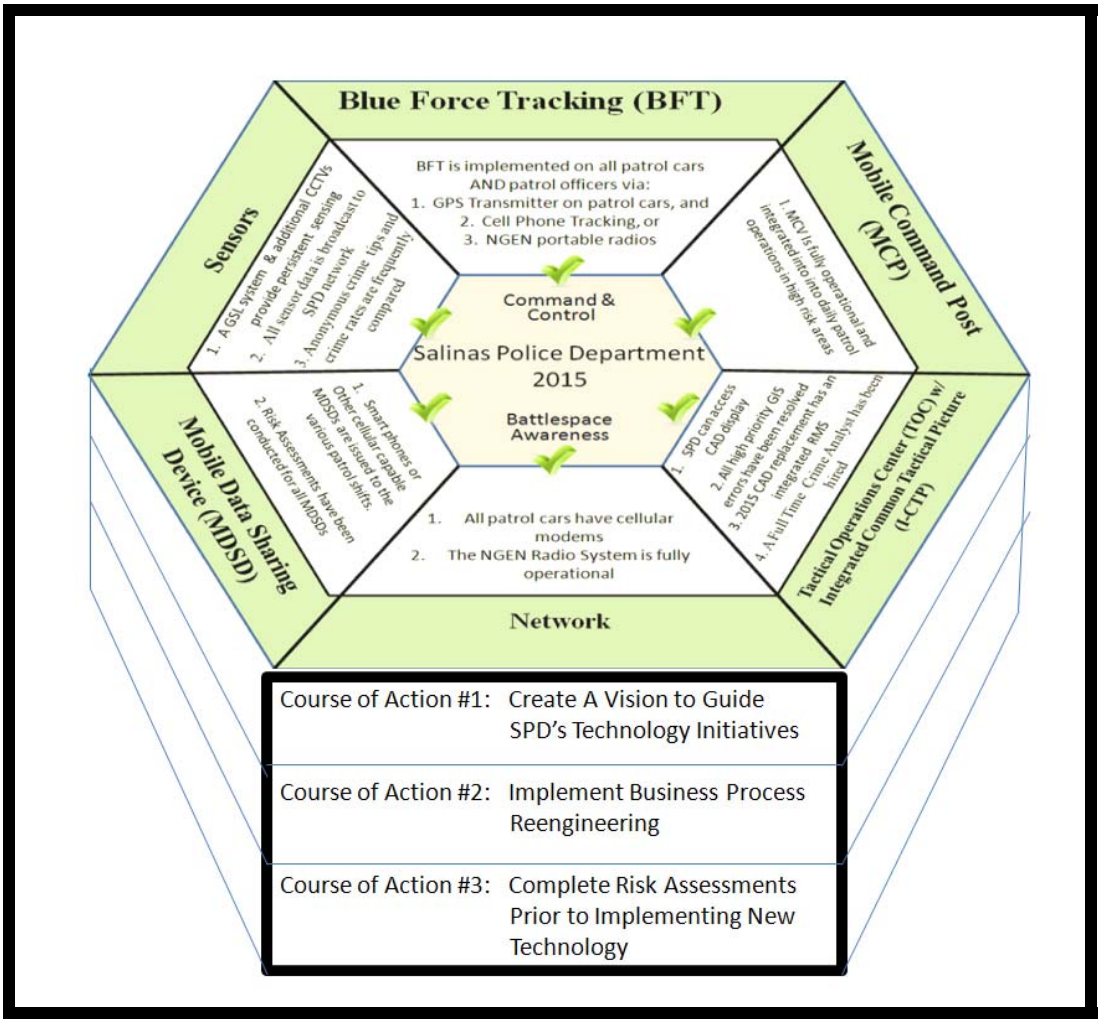


Figure 35. Visual Rendering of the Courses of Action As They Relate to the Technology Implementation Plan.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS

A. COURSE OF ACTION #1—CREATE A VISION TO GUIDE SPD'S TECHNOLOGY INITIATIVES

The first recommended course of action for SPD is to create a vision statement. Based on SPD resource constraints, the continued threats posed by gangs, and the planned implementation of several technological capabilities, a vision is needed to guide SPD from its present capabilities to a future improved state. A vision statement depicting the ideal end state will require the participation of all members of SPD so they can better visualize those actions that will be most supportive of SPD during this process of major technological change. A vision statement will ensure SPD makes best use of all available resources, unifies employee efforts to a common cause, and provides a common goal that all members can help achieve. Collectively this will maximize SPD's crime fighting potential during a time of significant change.

This vision statement can be incorporated into the SPD Chief of Police's Vision or become an entirely separate vision, such as a Capabilities Transformation Vision or an Information Technology Vision. In addition, this vision would provide SPD a chance to demonstrate those standards published in its value statement on the SPD website (Salinas Police Department, 2011). Figure 36 shows how the values of SPD can provide the central link between a current SPD vision and SPD 2015, the desired future information and communications architecture.

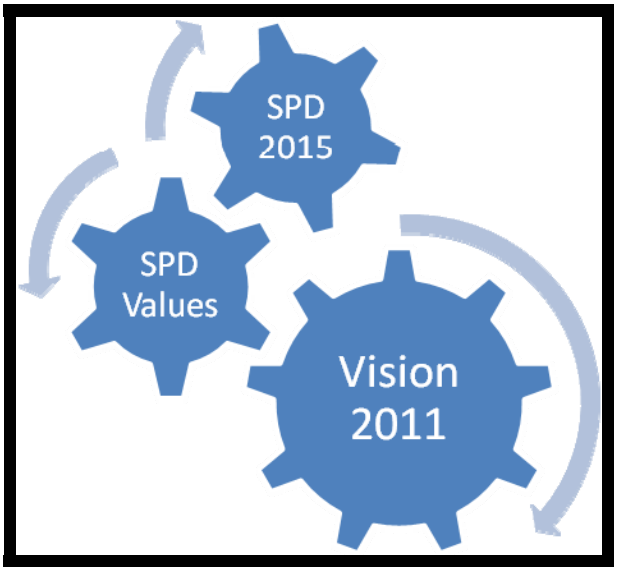


Figure 36. Use of a Vision Statement to Achieve SPD 2015.

In parallel to the SPD IT improvement effort, the State of California is undergoing a multi-year effort to improve its own IT infrastructure. This initiative started with a vision of implementing a *world class* IT program (California, 2011). To accomplish this, the Chief Information Officer (CIO) of California created an IT Strategic Plan that details the necessary changes needed to improve the State's uses of IT. While SPD and the State of California are very different organizations, the three goals listed in the state's Strategic Plan relate directly to many of the IT needs of SPD. The goals of the Strategic Plan are listed in the left column of the table below opposite SPD's IT needs.

California Information Technology Strategic Plan Goals	**SPD's IT Needs**
• Make Government Transparent, Accessible, and Secure • Drive Innovation and Collaboration • Make Information Technology Reliable and Sustainable Through Consolidated Platforms and Shared Services.	• Implement Secure Communications (NGEN) and Mobile Data Sharing Devices (iPod Touch) to combat Gang violence • Support Joint Operational Capabilities and Information Sharing (NGEN) • Connect Isolated Systems (Mug shot and Fingerprint Databases), Internet access to vehicles, and 2015 CAD replacement

Table 15. Comparison of California's Strategic Goals and IT Needs of SPD.

SPD can use the California Strategic Plan as a template to ensure its vision is in alignment with the current efforts of the State of California.

Finally, regardless of vision type, the ability of SPD to successfully implement its plan will be significantly influenced by both IT capabilities and current business processes. For example, if a specific vision is not supported by an appropriate IT systems or business processes, changes will need to be made in one or both areas. Depending on the amount of change needed this could impact SPD's ability to achieve its vision in the short term. Table 16 identifies how vision focus areas are impacted by both IT systems and business processes.

Vision Focus Areas	IT System needed to Support Vision	Possible Business Process Implications
Reducing Gang Violence	Fully integrated systems with push, pull, & share capability.	High level of process integration and standardization.
Joint Operations	Databases are accessible to a wide community of users. XML based technologies, P. 25 compliant radios, etc.	Increased participation in regional events.
Incident Response Time	100% communications coverage in all patrol areas.	Patrol strategy devised around times of highest activity. Resource staging to include use of Mobile Command Vehicle (MCV).
Public Perception	Mobile platforms support patrol officers while away from vehicles to allow increased interaction with the public.	Multiple patrol officers patrolling the same beat to allow for increased direct interaction with the public.
Metrics	Computer Aided Dispatch (CAD) w/ integrated records management system (RMS) and Full Time Analyst to synthesize sensor data into actionable intelligence.	Data driven policing strategies, Heat Maps, frequent changes to ops in response to new trends.

Table 16. The Impact IT Systems and Business Processes Have on Vision Focus Areas

Course of Action #1: Create a Vision to Guide SPD's Technology Initiatives

Create a vision to guide SPD's capabilities transformation from its present state to the recommended "SPD 2015" JBAIIC architecture.

B. COURSE OF ACTION #2—IMPLEMENT BUSINESS PROCESS REENGINEERING

The capability gaps identified in the architectural assessment combined with SPD's reduction in resources have greatly reduced any slack in the operational and responsive posture of SPD. In such an environment, Business Process Reengineering (BPR) can create resource opportunities but, to do so, requires evaluating all current business practices. Upon completing Course of Action #1, SPD should implement BPR as a way to extend the effectiveness of its current capabilities.

BPR is defined as the "radical redesign of age-old process[es] in the quest for significant improvement in performance" (Teng, J. Grover, V. and Fiedler, K., 1994). The purpose of BPR is not optimization such as happens when existing processes are left intact but computers are used to speed them up (Hammer, 1990). According to Hammer, BPR cannot be meticulously planned or accomplished in small groups taking cautionary steps. Rather, it is "an all or nothing proposition" where old assumptions are challenged and all processes are modified in favor of new ways of doing business (Hammer, 1990). For SPD, the upcoming implementation of new technologies offers an excellent time to evaluate existing processes to determine where improvements can be made.

SPD relies on many processes in the performance of its daily responsibilities; several of the processes frequently used by patrol officers are identified in Table 17.

Internal Processes (IP)	External Processes (EP)
1) Creating various reports 2) Filling out forms 3) Processing Field Interview (FI) cards 4) Processing evidence 5) Accessing information: a. while in the patrol car b. while at the office c. from Internal Databases: (fingerprint, mug shot, etc.) 6) Sharing information internally 7) Planning operations	1) Traffic enforcement 2) Incident response 3) Arresting people 4) Filling out FI Cards 5) Identifying people: a. Suspicious persons brought in b. Charged suspects 6) Moving people: a. Victims who can identify perpetrators from mug shots b. Persons of interest, criminals, etc. 7) Sharing information externally

Table 17. Frequently Used Internal and External Operational Processes.

In many instances, a process will require other processes to be initiated in order to be completed. For example, arresting a person (EP # 3) involves EP #4, #5, and #7 (table 14) at a minimum, in addition to potentially using all of the Internal Processes listed above. Recognizing how these processes interact with each other can lead to dramatic improvements. Finding a more efficient way to complete one process could provide significant time or cost savings to all interconnecting processes. For example, after an individual is arrested (EP #3), patrol officers may have to manually reenter basic case information (Name, Date, etc.) on as many as five different forms (IP #2) (Officer #1, personal communications, May 16, 2011). Reengineering the existing process with technology that automatically enters this information on all required forms would not only improve EP #3, but also IP #3, #4, and #5, and possibly others. The time saved by patrol officers would create more time to patrol or work on higher priority tasks.

External Process #5, Identifying People, is another area where BPR could provide substantial savings. Due to the limitations of the Land Mobile Radio System, the patrol officers are not able to access their local mug shot database while on patrol. After a crime is committed, the only way to obtain a positive identification from a victim/witness is to either bring the victim to the station to review mug shots or have the officer return to the station, obtain mug shots, return to the site, and present them to the victim/witness.

Accessing this database from the patrol car would eliminate the need for patrol officers to return to the station providing significant savings in fuel while better utilizing available man hours.

Course of Action #2: Implement Business Process Reengineering

Evaluate internal and external processes to uncover potential resource savings.

C. COURSE OF ACTION #3—COMPLETE RISK ASSESSMENTS PRIOR TO IMPLEMENTING NEW TECHNOLOGY

Today's law enforcement agencies have more technology choices available to them than ever before and many of these technologies can provide significant capability improvements. Technologies such as a gunshot location system (GLS), and closed circuit TV (CCTV) cameras allow a small number of officers to provide a virtual police presence throughout a city. Figure 37 demonstrates how technology is utilized by a typical police department. Figure 37(a) shows how technology enhances the capabilities of patrol officers to effectively manage a larger body of work. Figure 37(b) shows the choices that face a Chief of Police with regard to implementing technology following downsizing.

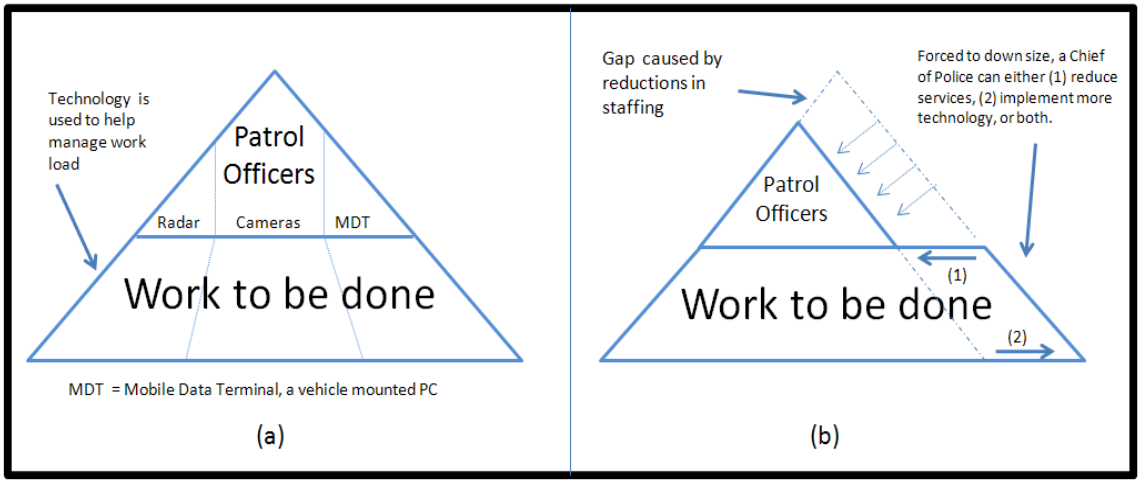


Figure 37. How Technology Is Used in a Typical Police Department.

Prior to implementing new technologies, SPD must assess the impact the technology will have on both existing business processes and its information and communications architecture. This evaluation is called a risk assessment. According to the National Institute of Standards and Technology, "risk" is defined as "the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (Stoneburner, Goguen, & Feringa, 2002). Currently SPD is planning to implement four unique technologies that have the potential to significantly reduce crime in Salinas. Each of these initiatives involves some measure of risk that upon implementation, could introduce vulnerabilities capable of adversely affecting the entire architecture. These risks and vulnerabilities must be understood. An April 27, 2011 announcement stated Apple's iPhone and iPad save the devices location is an example of how a technological capability could introduce vulnerabilities for law enforcement (Lowensohn, 2011). For example, these position files could reveal operational tactics such as patrol strategies that could be learned by others if an officer's device gets lost or stolen. While each of the initiatives SPD is implementing is state of the art, SPD's ability to accurately identify significant risks and vulnerabilities will ultimately determine whether these technologies enhance or reduce SPD's crime fighting capabilities. Additionally, the introduction of new technology might require either minor or major changes to business procedures within the agency in order take full

advantage of the technology (Maness, et al., 2001). By conducting risk assessments, managers at SPD will be able to view each technological initiative as it relates to the entire SPD organization and determine if appropriate safe guards are in place prior to implementing a new technology.

Finally, to ensure success with any integration effort, it is essential that all initiatives have both the commitment of senior management and cooperation of the members of the user community (Stoneburner et al., 2002).

Course of Action #3: Complete Risk Assessment Prior to Implementing New Technology

Implement technology risk assessments to limit organizational exposure to unknown threats and vulnerabilities.

VI. FUTURE RESEARCH RECOMMENDATIONS

This research revealed numerous opportunities for future research. Based on the results of the Architectural evaluation and the recommendations listed in the Technology Implementation Plan, the following researcher options provide the best opportunity to benefit SPD as well as other public safety organizations in Monterey County.

A. RECOMMENDED RESEARCH

- Monitor the implementation of ShotSpotter's Gunshot Location System and assess its effectiveness on reducing crime rates in East Salinas.
- Evaluate current business practices at SPD and determine which ones could best be reengineered with a technological solution.

B. ADDITIONAL RESEARCH OPPORTUNITIES

Due to the numerous technological initiatives currently underway at SPD, there exists ample opportunities to investigate how information technologies can enhance police officer effectiveness. Some research options include:

1. Technology

- The set up and technical configuration of a Tactical Operations Center at SPD.
- Configuring multicasting on the the existing CCTVs for viewing on patrol vehicles' Mobile Data Terminals.
- Analysis into which Computer Aided Dispatch system the dispatch center should implement in 2015.
- Analysis into how an integrated Records Management System could improve policing strategies at SPD.

2. Business Process Reengineering

- Determine more practical and secure uses for the iPod beyond that of a digital voice recorder
- Upon the completion of repairs to the Mobile Command Vehicle an assessment of the ways to improve its utilization.

- Evaluate the effectiveness of SPD's anonymous crime reporting methods and recommend methods to improve this sensing capability.

3. Research External to SPD

- Compare the estimated contractor costs to correct the digital maps used by the dispatch center with other mapping solutions to determine which could provide the accuracy needed to support the public safety organizations of the Monterey County at a reduced cost.

Various public safety organizations in the Monterey County are using different technologies for the same purpose. For example, the Pebble Beach Fire Department uses GST Mapper, by GeoSpatial Technologies, Inc., to maintain situational awareness with regard to the location of its fire engines. The Salinas Fire Department, on the other hand, uses a mobile version of Tiburon's Computer Aided Dispatch system. Research to identify other similar uses of technologies among the various public safety agencies in Monterey County could provide improved situational awareness for agency officials at significant cost savings.

C. CONCLUSION

This thesis introduced the JBAIIC architectural model as a way to improve the Salinas Police Department's ability to achieve command and control (C2) and situational awareness (SA) while combating violent crime. This architecture has been successfully implemented by Seal TEAM Eight to support counter insurgency operations in the Middle East. Similarities between insurgents and domestic gangs made the JBAIIC architecture an appropriate tool to use by domestic law enforcement agencies. Using the JBAIIC model, researchers identified the information and communications capabilities of a typical gang and showed that when a gang can access and share information more efficiently than law enforcement agencies, it creates significant opportunities to coordinate and execute illicit criminal activities. After completing a field demonstration, researchers analyzed SPD's information and communications architecture. This analysis identified significant capability gaps and showed SPD's current architecture is not capable of achieving the C2 and SA needed to effectively combat gang violence.

Recommendations were made to assist SPD in closing each identified gap. Finally, due to the significant resource constraints facing SPD and the planned implementation of several technological initiatives, a Technology Implementation Plan (TIP) was included as part of this thesis. The TIP identified how each of SPD's technological initiatives would impact its JBAIIC architecture and then concluded with three courses of action for SPD. Following these courses of action will allow SPD to more effectively use existing capabilities while ensuring future technologies are implemented in such a way to ensure long term benefit to SPD and Salinas.

This thesis explored the following questions, and provides in summary, the following findings answered the flowing questions:

- How can elements from the JBAIIC test bed knowledge base be adapted to the existing information architecture used by SPD to enhance its crime fighting strategies? *Demonstration #1 showed how implementing a Common Tactical Picture that utilizes Blue Force Tracking can significantly improve SPD's ability to achieve C2 and SA.*
- How will members of SPD successfully implement the JBAIIC architecture? *SPD 2015, the recommended future architecture for SPD in conjunction with the three courses of action, will allow SPD to implement a JBAIIC architecture.*
- How could other municipal governments facing similar issues with high crime and constrained resources apply the architecture created for Salinas to extend the effectiveness of its police force? *Figure 1 and Table 4 identify the JBAIIC architectural model and the essential characteristics of each architectural element respectively. Any agency facing similar resource constraints and high crime could use these tools to assess its own architecture to identify potential capability gaps.*

The Salinas Police Department will continue to face many challenges as it adjusts to recent reductions in sworn officers, fiscal constraints, and a deeply entrenched gang population. In an effort to remain effective as a law enforcement agency SPD must embrace a new way of how its technological capabilities are used in the fight against crime. By implementing a JBAIIC architecture SPD can most effectively combat Salinas' longstanding problems of crime while efficiently integrating new technological capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. SPD PATROL BEATS

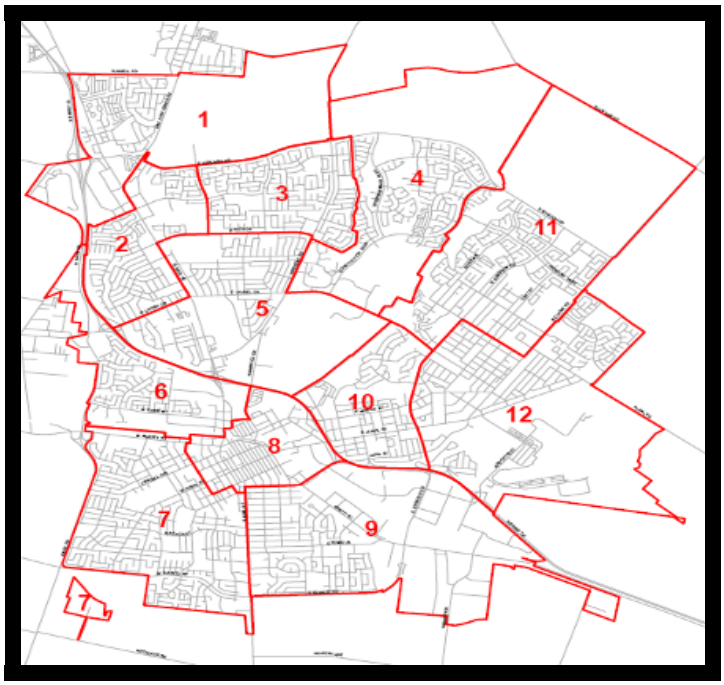


Figure 38. SPD Police Beats

Figure 39. Salinas, California Aerial View (From Google, 2011)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arnold, L., O'Gwin, C., & Vickers, J. (2010). *SMALL TOWN INSURGENCY.* U.S. Naval Postgraduate School).

Bercovici, M. (2006). FCC Narrowbanding Mandate: A Public Safety Guide for Compliance. *2006.*

BFT. (2011). *DoD dictionary of military and associated terms.* Online at: http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=battlespace+awareness&zoom_sort=0&zoom_per_page=10&zoom_and=1

Common Tactical Picture. (2011). Online at: http://www.dtic.mil/doctrine/jel/doddict/data/c/19014.html

Dept of Justice. (2009). *National violent crime rates.* Retrieved from Salinas, California

Fetherolf, L. (2010). *Report to the community.* Salinas, California: Salinas Police Department.

Garza, V. (2009). *SNS architecture EC 2009.* Naval Postgraduate School:

Hammer, M. (1990). Reengineering work: Don't automate, obliterate. *Harvard Business Review,* 1–8.

Irvine, N. (2009). *Empire challenge analysis report 2009.* Unpublished manuscript.

Kulkarni, A. B., Malaiya, Y. K., & Jayasumana, A. P. (1989). MESHNET: A New Fault-Tolerant LAN for Industrial Environment. Paper presented at the *Industrial Electronics Society, 1989. IECON '89, 15th Annual Conference of IEEE,* 537–542 vol. 3.

LeCappelain, J. (2010). *JBAIIC Hits the Ground Running at EC 10.* Online at http://www.jfcom.mil

Long, J. E. (2010). *A social movement theory typology of gang violence*. Monterey, California: Naval Postgraduate School. Online at: http://edocs.nps.edu/npspubs/scholarly/theses/2010/Jun/10Jun%5FLong.pdf (589.90 KB); http://handle.dtic.mil/100.2/ADA524726

Lorentz, R. (2010). *Understanding gang violence: Creating a Course of Action for Peace in Salinas, California.* Unpublished manuscript.

Lowensohn, J. (2011). *AG Wants Answers on Tracking from Apple, Google.* Online at: http://news.cnet.com/8301-27076_3-20057176-248.html?tag=mncol;txt

Maness et al. (2001). *A guide for applying information technology in law enforcement.* No. NCJ 185934).National Institute of Justice.

Markovic, J. Bueermann, & K. Smith. (2006). *Coming To Terms with Geographical Information systems.* Online at: http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=909&issue_id=62006

National Gang Intelligence Center. (2009). *National Gang Threat Assessment 2009.* Online at: http://www.justice.gov/ndic/pubs32/32146/activities.htm

NCH. (2011). *iPhone pocket dictate voice recorder – dictation software app.* Online at: http://www.nch.com.au/pocket/index.html

P25 Compliance. (2006). P25 compliance assessment program – fact sheet. *2006,*

Push. (2011). *The tech terms computer dictionary*. Online at: http://www.techterms.com/

Roeting, W. (2010). *Briefing to Commodore Szymanski.* Unpublished manuscript.

Salinas California. (2011). *(n.d.). in Wikipedia.* Online at: http://en.wikipedia.org/

Salinas Police Department. (2011). *Salinas police department - www.salinaspd.com*. Online at: http://www.salinaspd.com/

Solana, K. (2011). *Salinas Faces $7 Million Deficit.* Online at: http://www.thecalifornian.com/article/20110124/NEWS01/110124014/Salinas-faces-7-million-deficit

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* No. 800-30). Gaithersburg, MD: National Institute of Technology.

Teng, J. Grover, V. & Fiedler, K. (1994). Re-engineering Business Processes Using Information Technology. *Long Range Planning, 27*(1), 95–106. INITIAL

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Salinas Police Department
   Attn: Chief of Police
   Salinas, California

4. Dr. Douglas J. MacKinnon
   Naval Postgraduate School
   Monterey, California

5. United States Coast Guard Headquarters
   Washington, D.C.

6. Mr. Brian P. Wood
   Naval Postgraduate School
   Monterey, California